Intelligent management solutions
White paper

Tivoli. software

Providing highly secure access to information across government organizations.

*By Siddharth Bajaj, VeriSign Security Services Architect;
Michael Barton, IBM Network Security Solutions;
Beth Brownhill, IBM Government Solution Architect; and
Dave Hemsath, IBM STSM, CISSP, Security and Privacy*

August 2004

Contents

Executive summary

In a connected world, secure communication networks are essential to safe, reliable and efficient commercial, governmental and other societal transactions. Terrorist attacks on the United States have underscored the need to improve network security to access and share critical information among agencies and governments. Some of the factors at play in the area of government information access include:

- *The need for easy access to some government information as individuals can now get with private-sector information.*
- *Developing more-efficient processes to help lower costs and more effectively provide secure services to citizens, businesses and other government agencies, even as IT budgets tighten.*
- *Handling the public sector's renewed interest in security and vulnerabilities (weaknesses in systems, processes or the people who use them). Officials are looking to industry leaders – and new technologies – to more quickly identify threats, help authenticate identities and authorize access. Law enforcement, immigration and defense agencies are already using data mining, social-network analysis, profiling and biometrics. Knowledge-management tools make it possible for investigators to more effectively share information to create a full picture of risks.*
- *Maintaining awareness about the vulnerabilities created by increased dependence on information systems – particularly those accessible by malevolent hackers.*
- *The need for governments to deliver on policies that require them to more effectively prevent or respond to threats.*

IBM offers solutions for the government sector that provide highly secure information access for citizens, businesses and cross-government interests. This paper covers some of the business processes and solution architectures that both agency directors and technical architects might consider for deploying secure, networked solutions. These individuals can use currently available solutions as-is or as building blocks to provide agencies with solutions that can help support:

- *Secure electronic forms and records management.*
- *Secure access to government information and services.*
- *An on demand workplace.*
- *Interagency and intergovernmental collaboration.*
- *Public safety initiatives.*

IBM and VeriSign – a provider of critical infrastructure services that help make the Internet and telecommunications networks more intelligent, reliable and secure – along with leading IBM Business Partners, provide security rich solutions that can help governments share information. They, in turn, can help make information available to authorized governments, agencies, businesses, employees and constituents while helping to maintain confidentiality, integrity and availability requirements.

This paper uses solution patterns and best practices learned from securing private enterprise and government environments. These provide the basis for government-solution IT architects to design and integrate solutions for highly secure access to information between government organizations, businesses and citizens.

Security basics

Some private enterprises fully understand information security principles and risk management. The corresponding government principles in the area of risk are discussed in the U.S. Federal Information Security Management Act (FISMA) of 2002.[1] Government agencies can identify and provide information security protections (that is, policies, procedures and technology) that are commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of:

- *Information collected or maintained by, or on behalf of, an agency.*
- *Information systems used or operated by an agency, by a contractor of an agency or other organization on behalf of an agency.*

Security

Security is neither a product nor a service. It's a condition. The *American Heritage Dictionary* defines the condition of security as "freedom from risk or danger" and "freedom from doubt, anxiety or fear."

Security is never absolute. There's no such thing as complete safety, or complete freedom from doubt or fear; people and organizations always face risks. Some risks can be eliminated, some can be reduced and others just have to be tolerated. You typically feel secure when you understand and can manage the level of risk you face so that it is acceptable when measured against the ease of moving through the world.

Risk

Risk is a factor or course involving uncertain, likely unforeseen, danger. Organizational risk is the potential that something negative will happen to the organization. There are many different types of risks:

- Asset *risk is the risk of theft, destruction or vandalism.*
- Identity *risk is the risk of impersonation.*
- Infrastructure *risk includes network infrastructure risk (passive and active wiretapping, denial of service) and system infrastructure risk (subversion, denial of service).*
- Operational *risk is the risk that internal processes and procedures will result in financial losses.*
- Custodial *risk is the risk of failure to protect others' assets.*
- Compliance *risk is the risk that a business will fail to comply with laws and regulations.*
- Credit *risk is the risk that parties in a contract will not meet their financial obligations.*
- Market *risk is the risk that a business's assets will lose value because of changes in market conditions.*
- Information *security risk is the risk that exploiting a vulnerability in the information systems of a business will result in a financial loss.*

Typically, business risks are quantified in economic terms, so a business risk is based on the possibility that an event will decrease the economic value of the business to its owners. Government risk can span from fraud, economic loss to a community or the nation, to a catastrophic breach of national security. Risks are quantified using a simple formula that calculates the expected loss that a risk creates. The formula is:

Risk = Probability x Consequence
where *Probability* is the likelihood that a specific negative event will occur at some point in time, and *Consequence* is the economic loss that will occur if the negative event happens.

Businesses manage risk in a variety of ways:

- Transference. *A business can transfer risks to other parties. A warranty, for example, transfers the risk of a product failure from the product's buyer to its seller.*
- Indemnity. *A business can recover the cost of a risk through arrangements with third-party risk specialists. An insurance policy, for example, allows the policyholder to recover the cost of losses covered by the policy's terms from the insurer.*
- Mitigation. *A business can reduce risk either by reducing the probability that an adverse event will occur or by reducing the consequences that will result from the event's occurrence. For example, a business can reduce fire risk by adhering to the electrical code—reducing the probability of a fire—or by installing sprinkler systems that reduce the damage that a fire will cause.*
- Avoidance. *A business can choose not to engage in activities that create certain types of risks. For example, an electric utility might choose not to construct nuclear power-generating facilities if it believes that the risk associated with environmental regulations is too costly.*
- Acceptance. *A business can choose to live with the consequences of a risk. Normally, a business will choose this option only if the risk has a low probability, low consequence, or both. A business that chooses to accept risks often sets aside resources to offset risk-related losses; this is called* self-insurance.

Vulnerabilities, threats and countermeasures

If information systems were always perfectly suited to their tasks and could not be made to perform improper functions, and if people never made mistakes and information-handling processes were always correctly designed and effective, information security risk would be dramatically reduced. Unfortunately, systems contain design and implementation flaws, people make mistakes and processes are not perfect. These vulnerabilities create the possibility of a system failure, which, in turn, creates the possibility of a service loss.

Vulnerabilities alone do not create risks. Vulnerabilities can exist in a system for a long time without causing failures or losses. Vulnerabilities can contribute to system failures in several ways, including:

- *Accidents. When the system is vulnerable, events or user actions can trigger a failure.*
- *Attacks. If the attacker knows about the vulnerability and how to exploit it, he or she can deliberately render the system vulnerable and intentionally trigger a failure.*

Although accidents are not usually considered security failures, successful attacks are. A successful attack requires two ingredients: a vulnerability, and a capable, motivated attacker, called a *threat*. The risk of a security failure is defined by the following formula:

$$\textit{Security Risk} = P(t,v) \times C(v)$$

where $P(t,v)$ is the probability that a particular threat (t) will exploit a particular vulnerability (v), *and* $C(v)$ is the consequence of successful exploitation of vulnerability (v).

Security risk can be managed using any of the risk-management mechanisms described in “Risk” on page 4.

When a business chooses to mitigate security risk, it does so by implementing countermeasures. A countermeasure is an action taken to significantly reduce or eliminate the probability that a vulnerability can be successfully exploited or to reduce the consequences of successful exploitation of a vulnerability.

Examples of countermeasures include:

- *Distributing a software patch to fix a programming error.*
- *Installing a firewall to make it harder for attackers to connect to a business's systems.*
- *Installing an intrusion-detection system to make it more likely that an attack in progress is quickly detected and eliminated.*

Mitigation

A critical factor in mitigating physical and information security risks is time. Given enough time, a dedicated attacker with good access to resources will eventually find and exploit a vulnerability in any system. The key to defeating attacks, therefore, is to detect these attacks before they succeed, and respond in a way that convinces or forces the attacker to give up the attempt.

Because mitigating security risks is a time-driven process, it can be divided into the four phases of the information security risk-management life cycle:

Assess. In the *first phase* of the cycle, the business catalogs assets, identifies the value of each asset, identifies system vulnerabilities and threats, estimates the probability of exploitation of vulnerabilities by threats and identifies the consequences of exploitation of each vulnerability. This process is called *risk assessment.*

Protect. In the *second phase* of the cycle, the business deploys countermeasures to protect against successful exploitation of vulnerabilities.

Detect. In the *third phase* of the cycle, the business continuously monitors the operation of its systems to detect attempts to exploit vulnerabilities.

Respond. In the *fourth phase* of the cycle, the business responds to detected attacks by reconfiguring systems, recording data necessary for prosecution or other actions, minimizing and containing any damage resulting from partial or complete success of detected attacks, and restoring any damaged systems or assets to correct configurations.

Completing the assess-protect-detect-respond cycle quickly enough to detect and defeat attacks before they can cause damage is the key to successfully mitigating information security risk.

Protection

When deploying countermeasures to protect systems against attacks, governments need to understand what they want to protect against. Seven broad classes of countermeasures include:

- Authorization *countermeasures can protect against accidental damage, theft, destruction or vandalism of information assets. Access control systems are examples of authorization countermeasures.*
- Accountability *countermeasures help a government agency to determine who is responsible for actions that might affect its operations. Audit logs and digital signatures are examples of accountability countermeasures.*
- Authentication *countermeasures help protect against impersonation of users and usurpation of legitimate authority. Login passwords, smart cards holding digital certificates and associated private keys, and biometric authentication devices are examples of authentication countermeasures.*
- Data protection *countermeasures comprise two types:*
  - Confidentiality *countermeasures help protect against unauthorized disclosure of sensitive or classified information. Encryption is an example of a confidentiality countermeasure.*
  - Integrity *countermeasures help protect against unauthorized modification of information, the correctness of which is important to the operation of the government agency. Checksums and hashes are examples of integrity countermeasures.*
- System integrity *countermeasures help protect against corruption of the security services themselves. Antivirus utilities, signed code and intrusion-detection systems are examples of system integrity countermeasures.*
- Privacy *countermeasures help protect against improper use and disclosure of information about individuals. Privacy policy enforcement and auditing tools are examples of privacy countermeasures.*
- Availability *countermeasures help protect against interruption of services that the government agency or its clients depend on. Backups and redundant servers are examples of availability countermeasures.*

Levels of authentication strength

The U.S. Government Office of Management and Budget (OMB) has established guidelines defining four levels of authentication strength (confidence) based on the need to identify and authenticate users and other entities requiring identification and authentication (I&A).

- *Level 1: Little or no confidence in asserted identity—for example, self-identified user ID, password*
- *Level 2: Some confidence in asserted identity —for example, user ID, PIN or password provided by a recognized authority*
- *Level 3: High confidence in asserted identity —for example, digital certificate-based signing operations or use of a security token generator, or both*
- *Level 4: Very high confidence in the asserted identity—for example, multifactor authentication or hardware [including biometric] authentication devices, or both. An example of a multifactor authentication might be:*

  -Something you have—for example, a smart card

  -Something you know—for example, a PIN or pass phrase

  -Something you are—for example, fingerprint, iris pattern or voiceprint

An important requirement for a secure access control architecture is authentication to verify the identity asserted by a user. Other security countermeasures, such as authorization and auditing, depend on a user's identify being authenticated effectively.

Stronger mechanisms for identity authentication

The following mechanisms provide a higher level of security than passwords, especially when used in concert.

Digital certificates

Based on public key encryption, digital certificates serve as unique, unforgettable online credentials that authenticate the identity of each device or device user, and identify privileges to provide authorized access to private online information. Besides being a superior mechanism for identity authentication, digital certificates enable digital signing and encryption to provide the privacy, data integrity and nonrepudiation services.

Tokens and smart cards

Tokens and smart cards carry an embedded microchip that stores security data and applications. They hold more information than magnetic stripe cards and can be programmed for a variety of applications. Multiple applications can reside on a single token, and applications can be added, deleted or upgraded without reissuing the token. Requiring a PIN to access credentials on the token provides an added layer of protection if the token itself is lost or stolen. Tokens can also be used with biometrics such as palm, fingerprint or retinal scanning to strengthen security.

Digital certificates with tokens

Digital certificates combined with tokens offer greater security, convenience and portability for Internet-based communication and commerce than either a digital certificate or token alone. Placing the digital certificate on the token provides more protection against theft or impersonation than if it were stored on the user's hard drive. Networks, systems and applications are much less likely to be compromised. Also, by incorporating one or more identification certificates on the token, users have the appropriate credentials to access systems remotely, severing ties to a single workstation.

Digital certificates with TPMs

Trusted platform modules (TPMs) are isolated chips that reside on the computer's motherboard and use digital signatures to verify that the operating system and other components of the software environment have not been compromised. When combined with a digital certificate, they provide very strong authentication.

Assurance

Deploying countermeasures to mitigate risks helps contribute to the safe access to a government's information. As mentioned earlier, the definition of security includes more than safety—it also includes freedom from doubt, anxiety or fear. To minimize doubt, an agency must do more than manage risk; it must also build confidence that its risk-management regimen is effective. Building confidence in security risk-management measures—especially mitigation measures—is called assurance. Increasing confidence in a government agency's security regimen requires:

- *Testing it on a regular basis.*
- *Implementing appropriately strong I&A to establish trust, provide authorization and audit the system.*
- *Providing third-party analyses, audits and formal certifications.*
- *Adhering to standards of practice, technology standards and industry best-practice guidelines.*

Cost

Is security expensive? It depends. Because security is never absolute, managing security risks requires a cost-benefit calculation. If you have a lot of losses due to security failures, more security is not expensive—in fact, it might mitigate losses and save money. If you have a low risk of loss, then security is expensive because there is little financial benefit to balance the cost.

Quantifying the cost of security is tedious, but not terribly complicated; you have to add up not only the cost of acquiring technology, but also the costs of hiring and training staff and other life-cycle costs—and factor in the impact of security procedures on productivity. Quantifying the benefits of security is much more difficult, because you don't always find out about attacks that didn't succeed. And you can't know in advance whether your security is going to defeat an attack.

Beyond a certain point, security can often end up providing diminishing returns; investing more doesn't add significantly to existing safety features. As Figure 1 demonstrates, balancing the cost of effective losses and the cost of protection is more an art than science. And increasingly, managers have found that juggling these costs, while keeping the total cost low enough to make a profit, is an even tougher trick.

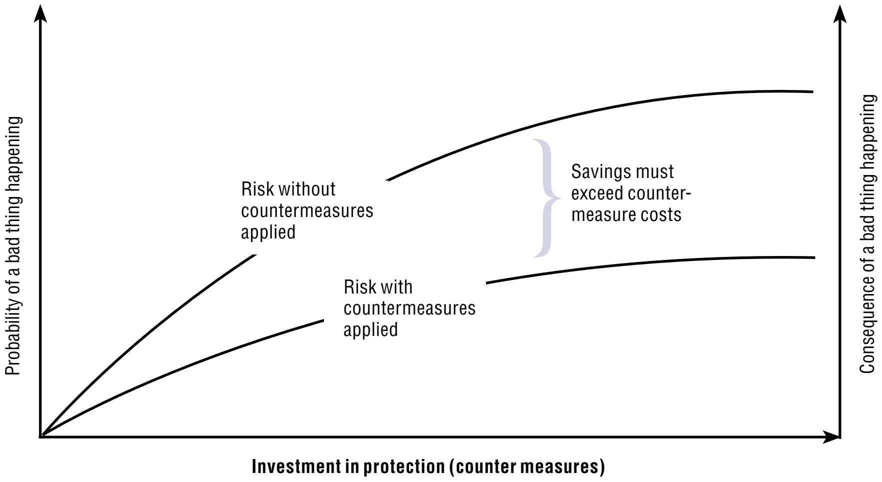

Figure 1. Security cost-benefit analysis.

Security challenges for government agencies

Governments around the world feel the pressure to meet the same on demand expectations and criteria as the private sector. Consumers expect governments to provide most of their services online and in near real time, while governments are looking for ways of reducing the total cost of providing these services. This e-government movement means that much more data, including personally identifiable information, is being stored on insecure networks, such as the Internet. The challenge for governments lies in making the required data and delivery of services to citizens, businesses and other government organizations more available while instituting the appropriate levels of security.

World governments are also faced with the challenge of moving from a traditional "need-to-know" mindset to a new "need-to-share" way of conducting operations to support local, regional, national and international security operations. This new model is characterized by more agile, dynamic and robust IT infrastructures.

Government agencies are increasingly subject to mandated information security requirements, especially in the area of assurance. For example, the U.S. military falls under U.S. Department of Defense Instruction 8500.1, which requires formal security evaluations of products and cryptographic modules deployed in Department of Defense systems. And the Federal Information Security Management Act (FISMA) of 2002 requires demonstrable improvement in information security each year.

Government agencies need to ensure that their systems comply with all relevant policies, regulations and laws. This compliance monitoring and enforcement should be as automated as possible to free up scarce human resources. Compliance tasks run the gamut from security-patch management to system configurations, records retention and protection policies, audits and reports.

Any IT program has a budget. Part of a government's approach to managing cost is to switch from government off-the-shelf (GOTS) systems, or systems developed for and purchased by governments, to commercial off-the-shelf (COTS) systems. Governments, like private-sector organizations, can cost-effectively provide security for their systems by properly understanding and managing the risk associated with them. A particular challenge for governments is the set of metrics and methodologies used to perform the cost-benefit analysis. Government agencies, for the most part, are not revenue- or profit-generating organizations. Well-understood principles of risk management help organizations to deploy security commensurate with the value of the assets at risk – people, data, IT equipment and so on – and the probability of an adverse event happening to one of them.

The following interactions between entities and government are defined based on private-sector on-demand business models.

- *Citizen-to-government (C2G) transactions, such as renewing a driver's license*
- *Business-to-government (B2G1) transactions, when the business is wholly within the government's jurisdiction—for example, state sales-tax transactions*
- *Business-to-government (B2G2) transactions, with the business spanning multiple governments' jurisdictions—for instance, transactions with an international shipper such as Federal Express or TNT Express*
- *Government-to-government intra-government (G2G1) transactions, such as those between organizations within the same government such as law enforcement, emergency response, and fire fighting organizations*
- *Government-to-government inter-government (G2G2) transactions involving peer levels within a hierarchy—for example, a transaction between law enforcement organizations in different governments*
- *Government-to-government (inter-government, hierarchy) (G2G3) transactions—for instance, those between a state police and the U.S. Federal Bureau of Investigation (FBI).*
- *Government-to-government (G2G4) transactions, with the government geographically spanning multiple government entities, such as interactions by a city covering two or more counties*
- *Government-to-government (G2G5) transactions, with inter-government peer levels without a hierarchy, such as first-responders incident response, information sharing or inter-agency emergency response management*
- *Employee-to-government (E2G) transactions for instance between field agents and the government*

Secure IT infrastructure and components

Government solutions are built around important business or organizational processes. They exist to enable governments to better fulfill their missions. When looking at system architectures for these solutions, it becomes evident that there are common, recurring elements across them. These elements aren't limited to these particular solutions or even the government sector. Instead, they're combined into repeating topology—the system's physical layout and the relationships between system components. A primary source for these pattern descriptions is the IBM paper, *Introduction to Business Security Patterns*.[2]

This paper focuses on the topologies employing Web browser-based user access to Web portal server-based resources. The principles shown in Figure 2 are easily extended to other environments and models, such as asynchronous messaging topologies. Figure 2 summarizes the general component-type relationships and the transport classifications to the network zones discussed later in this section.

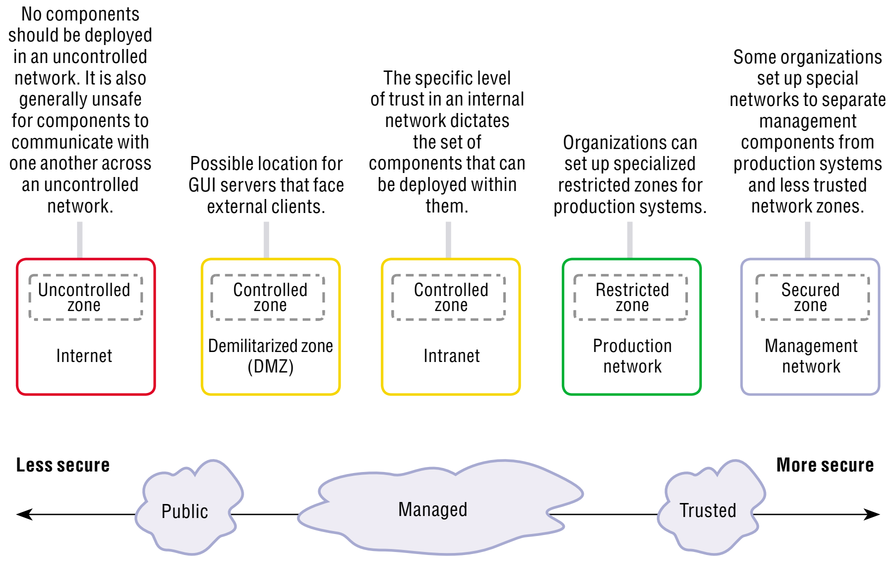
No components should be deployed in an uncontrolled network. It is also generally unsafe for components to communicate with one another across an uncontrolled network.
Possible location for GUI servers that face external clients.
The specific level of trust in an internal network dictates the set of components that can be deployed within them.
Organizations can set up specialized restricted zones for production systems.
Some organizations set up special networks to separate management components from production systems and less trusted network zones.
Uncontrolled zone
Internet
Controlled zone
Demilitarized zone (DMZ)
Controlled zone
Intranet
Restricted zone
Production network
Secured zone
Management network
Less secure
More secure
Public
Managed
Trusted

Figure 2. Graphic representation of network zones, transport classifications and their levels of trust.

Web presence

The simplest topology is Web presence, which is typically an Internet-based information portal or the dissemination of client-facing, non transaction-oriented organizational information. The goal of a Web presence is to provide Internet-based access to an organization's public information.[3] The value of the information derives from its integrity and availability. Web presence deployments do not ask for any client's personally identifiable information. However, best practices might include the use of Secure Sockets Layer, Version 3 (SSLv3) or Transport Level Security (TLS) software to protect the integrity of content in transit from the organization to its clients. Best practices dictate that the content should be static, without embedded programs such as JavaScript™, and without servlets or Java™ ServerPages (JSP) technology. However, most organizations choose to deploy one or more of these dynamic technologies to meet their mission requirements more effectively.

The goal of security is protecting the integrity and availability of the information that is disseminated. An organization has little control over the client-access points—Web browsers running on traditional personal computing devices or pervasive devices such as personal digital assistants (PDAs) and Internet-capable cell phones. Although the access point lacks security, risk is low because the information is public.

As part of the strategy to maintain the integrity and availability of the data and contain additional risks, many companies deploy defense-in-depth security barriers to create a neutral zone between an organization's intranet and an insecure network such as the Internet. The neutral zone is often referred to as a *demilitarized zone (DMZ)*. DMZs are bound by firewalls that protect the data and attempt to mitigate denial-of-service attacks. High-availability server solutions inside the DMZ also help mitigate availability risks.

Web presence presents a limited opportunity for attackers. The major risk for an organization using Web presence is harm to the organization's brand image and value. The threats include:

- *Unavailable data due to a denial-of-service attack or the destruction of the information being presented*
- *Altered or corrupted data, which might occur in a site defacement attack*

There are two subcategories within Web presence.

Isolation from the core organization

If the Web presence isn't connected to the organization's intranet, outsiders can't access systems that might contain more critical data. The only concern is the integrity and availability of the information provided (see Figure 3). The administrators responsible for the Web content maintain its integrity, following established procedures to sanitize and validate updated content and software – for example, running an antivirus scans on the files – before installing the updated content or software. They must go to the physically secure DMZ site to perform this operation, because no administrative network connection to the DMZ systems exists.

The best practice known as *hardening* also maintains the integrity and availability of the Web presence servers. Hardening includes turning off or uninstalling unneeded programs and accounts that can serve as attack vectors. It includes proper setting of the file permission bits on the programs and data, and might use other security products to enhance and enforce security capabilities of the environment's operating system platform. Multiple instances of the content being served to clients promote availability. A load-balancing program or appliance manages the multiple instances. The firewall filters out unsanctioned protocols.

In this topology, probably only HTTP, HTTP Secure (HTTPS) sockets and File Transfer Protocol (FTP) protocols are supported or allowed through the firewall. The firewall may be capable of inspecting the allowed protocol traffic and trapping malformed protocol flows. Working in conjunction with the firewall and the router, a monitor looks at inbound network traffic to detect and react to suspicious or hostile network activity.

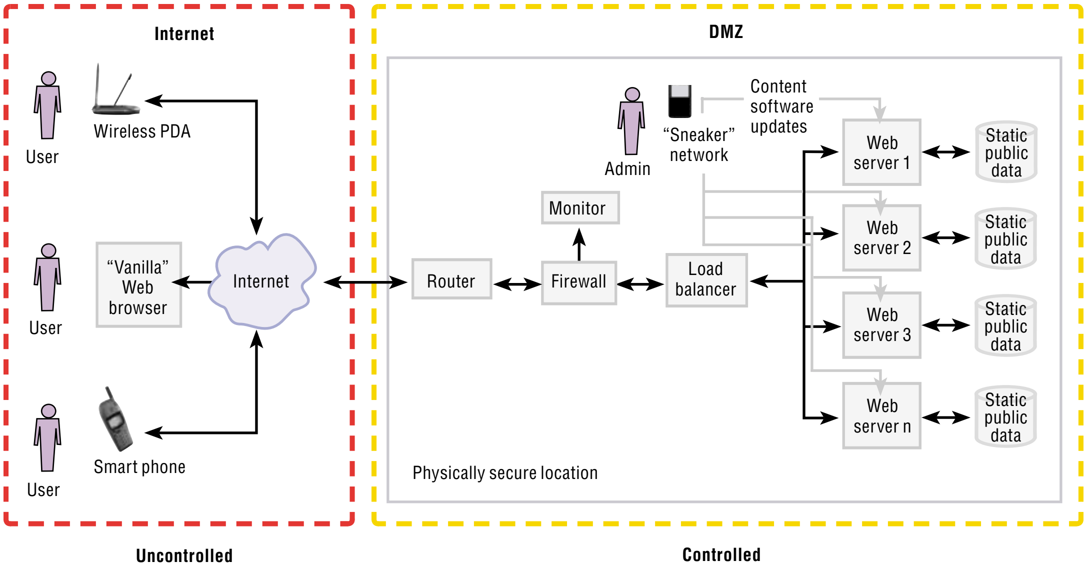

Figure 3. Web presence (isolated).

Integration with the core organization

If the Web presence is connected to the organization's intranet, security vulnerabilities might lead to unintended network and systems access. This collateral access can result in the need to manage other risks. Figure 4 shows the differences between this topology and that shown in Figure 3. The major difference is that administrators can now perform program and content updates remotely from within their secure management zones. This requires adding an interior firewall to the DMZ, which is configured to only accept initiation of approved secure protocols, such as Secure Shell, from the management zone. All communication channels used for transmitting information requiring integrity and confidentiality must be set up with one or more secure protocols such as Internet Protocol Security (IPSec), SSLv3 or TLS, Kerberos, or others. SSL and TLS are the most prevalent protocols for use with Web traffic. Web servers (and possibly the interior firewall) must identify and authenticate administrators.

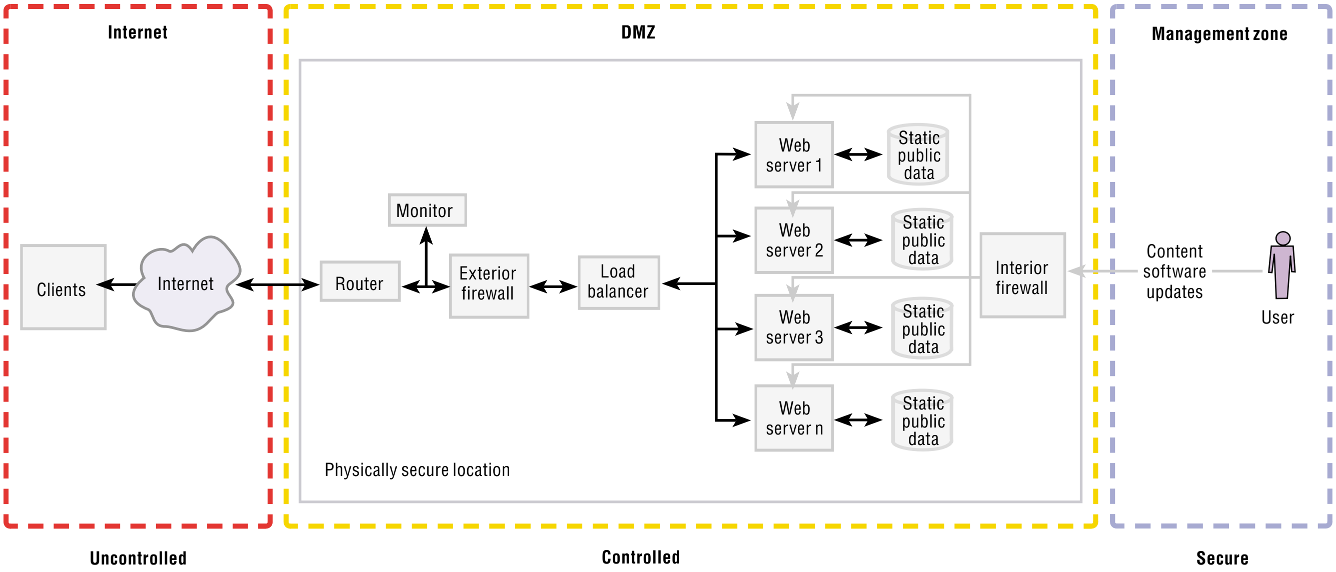

Figure 4: Web Presence (integrated).

Citizen-to-government (C2G)

The C2G topology deals with a government's ability to conduct transactions with or on behalf of its citizens over networked systems. C2G operations allow individuals to engage in online transactions and to manage data such as accounts, e-mail, collaboration, taxes and benefits.

A fundamental characteristic of the C2G topology is that the government agency or agencies must know the citizen involved in the transaction. Therefore, a registration process is required to establish each citizen's identity and what type of authentication to use. For low-value transactions with lower risk, an agency might allow a citizen to self-register or enroll online. For higher-value transactions such as student loan repayments, tax filing and benefit inquiries, government agencies need to have established policies and procedures for citizen enrollment – and out-of-band transmission of authentication information to registered citizens. Guidelines such as the aforementioned OMB publications help government agencies establish the robustness of the identification and authentication used for their C2G transactions. The assets associated with the C2G topology that need to be secured include:

- *Personally identifiable information*
- *Account access information*
- *Information presented to the user*
- *Links between the government entity and the citizen*

Aside from the user's identity, the C2G topology has other, specific basic attributes. C2G transactions involve the exchange of personal information, financial data and personalized subscription-based information. For this reason, a government entity should provide transaction-based protection of data and identities. The value for any one transaction is limited, while the accuracy is important. Any one transaction is not a major risk, but, collectively, the loss or misuse of data can seriously affect citizens' trust in the government entity or the government as a whole.

The major threats in the C2G topology are impersonation, collateral access to government systems, misuse of personal data, unauthorized modification or destruction of data and unauthorized disclosure. These threats can originate from inside or outside a government entity. The simplified reference topology for C2G is shown in Figure 5.

The C2G topology builds on the Web presence topology. There are two classes of users, citizens and employees (regular and contracted).

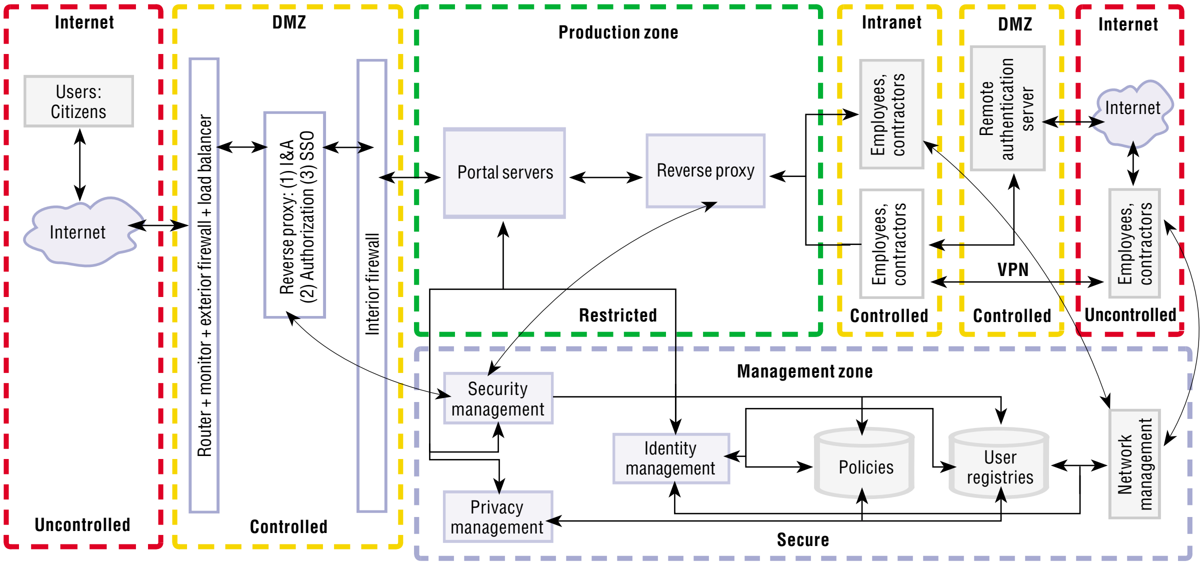

Figure 5. C2G topology

Citizens

Because citizens need access to production data, transactions and other information, they must now identify and authenticate themselves to the IT systems that serve them. This is the role of a new element in the DMZ, the *reverse proxy*. The reverse proxy looks like a Web server to the citizens, and it looks like a standard Web browser to the portal servers in the production zone. It moves the requests between users and the portal servers, in a manner that is transparent to both.

The reverse proxy shown in Figure 5 performs multiple functions, including:

- *Identifying and authenticating users.* The I&A function must be flexible and robust, capable of supporting multiple levels or types of identification and authentication that the OMB requires. The government organization can choose the levels of authentication needed based on the required levels of strength of security required for different applications (refer to the Levels of authentication strength sidebar for more details).
- *Authorizing users to specific resources.* Authorization is independent of identification and authentication. The reverse proxy functions as an access enforcement function (AEF), defined in the International Organization for Standardization (ISO) 10181-3 Authorization Model, as shown in Figure 6. The security-management component in the management zone functions as the corresponding access decision function (ADF). Note that for purposes of clarity, specific performance-enhancing measures, such as local caching of key information are not shown in Figure 5. Figure 7 shows more detail for the ADF, which enables robust policy support. This model supports multiple access control policies with no changes to the AEF's core logic. Therefore, a policy for Role-Based Access Control (RBAC) can be supported along with other policies.

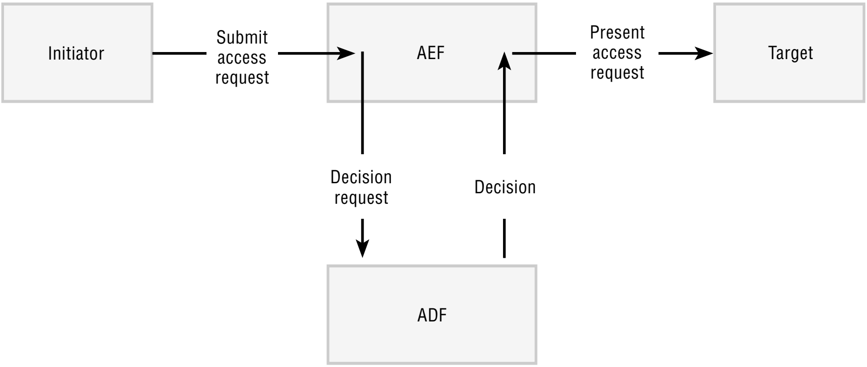

Figure 6. The ISO 10181-3 Authorization Model.

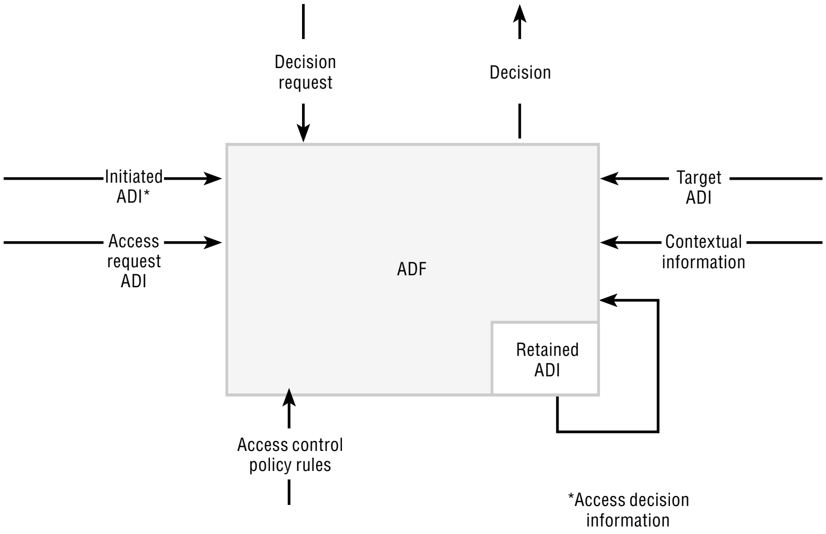

Figure 7. The access decision function.

- *Providing single sign-on (SSO) to resource managers.* A single sign-on allows a user to sign on one time, eliminating the need for repeated authentication and simplifying access to multiple applications and tools. Single sign-on uses the strength of strong authentication and access management to protect authorized access and use of government information. This occurs behind the portal servers, which are not shown in Figure 5.

Employees and contractors

In cases where users are agency employees, a different set of considerations and corresponding policies must be implemented. These users' information resides in the controlled environment of the organization's intranet. Each employee must go through an I&A process at his or her workstation. However, because insider attacks can be equally or more damaging than attacks from outside an organization's security perimeter, organizations can deploy a separate internal reverse proxy to control employees' Web-based access to production resources.

Employees working at home, or outside an organization's security perimeter must first authenticate to a remote authentication service. This service is used to establish a virtual private network (VPN) connection that logically places them inside the organization's intranet, indistinguishable from "local" users.

Other elements in the management zone include:

- *The privacy-management element, which deals with enabling appropriate controls around personally identifiable information.*
- *The identity-management element, which is the master provisioning engine for creating, modifying and revoking identity account and credential information for users and resources, including data, applications and networks.*
- *The security-management sub element that deals with the event data generated by sensors, auditing daemons and other means. This sub element, acting on the organization's policy, collects and analyzes data, filters out low-impact and false-positive events, and presents high-impact events to operations staff for appropriate action.*
- *The network-management element enables more defense-in-depth security barriers by first authenticating hardware devices to a network before allowing any higher-level network access by software. Organizations can apply this to both the local and remote instances of employees and other users.*

Although not shown in Figure 8, there are other management and operational elements that cross the zones, depending on specific needs. These include directories such as Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP), X.500 and Network Time Protocol (NTP) time sources.

Business-to-government (B2G)

B2G interactions involve secure government transactions with single or multiple businesses. Typically, the transaction occurs under a contractual relationship – set by the participating government agencies – among the appropriate parties. These include either explicit or implied agreement among the parties on risk, mitigation and liability. The goal of the B2G pattern is to provide an efficient and secure information exchange within a trusted relationship. The participating government entities establish the appropriate business registration process and how credentials are issued. Some of this process can be outsourced for lower-value transactions.

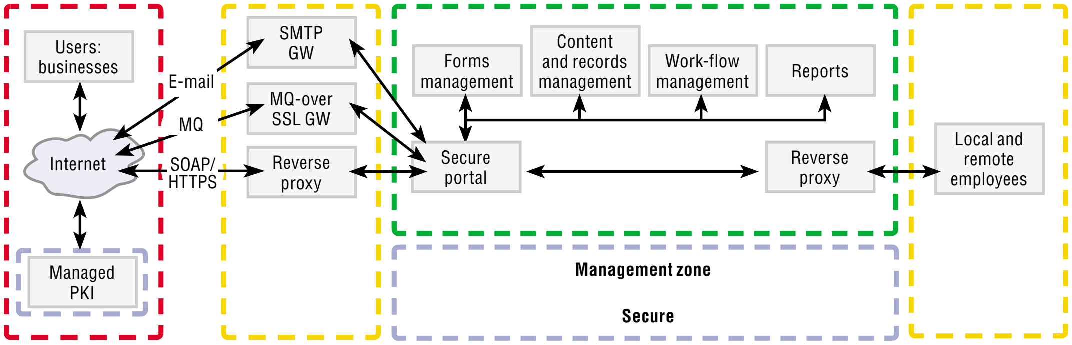

Figure 8. B2G topology.

The B2G topology introduces new transaction paths. Besides browser-based transactions, B2G allows for asynchronous, message-based transactions, such as e-mail and message queuing. These transaction types might not make use of workflow technology to automate their processing. Even if an agency operates its own public key infrastructure (PKI) management elements, such as registration authority (RA) or certification authority (CA) within its internal management zone, these elements logically appear to be based in and accessible from the Internet zone.

The three categories of B2G relationships include:

- Simple supplier. *In this relationship, a business communicates to a government entity to transact business. The data shared is not sensitive (for example, ordering information), so it might not be encrypted. Security, as an embedded attribute of B2G relationships, is employed to help ensure that the government entry point is protected from unwanted intrusion attempts or malicious code entering the infrastructure.*
- Trusted supplier. *With this relationship, the sensitivity and value of data tends to be higher than that of a simple supplier relationship. An example of a trusted supplier would be a business communicating tax information or making payments to the appropriate government agency or agencies.*
- Partnership. *In this relationship, the sharing and collaboration of data leads to increased security exposures in the IT infrastructure that must be managed.*

All of these relationships lead to common security exposures, which the government entity can mitigate with effective countermeasures. Intrusion detection systems, firewalls, authorization and access control systems, and separation of content tools are generic security components that implement countermeasures. The increasing sensitivity of data in a trusted supplier relationship or partnership may escalate the need for VPNs, secure e-mail and independent third-party audits.

Government-to-government (G2G)

As shown in Figure 9, there are two[4] methods of connecting the IT systems of two or more government agencies. The first method uses dedicated (or isolated), trusted internetworking connections. This method is frequently used for the most sensitive or classified systems. The second, more-common method is to establish a VPN across an insecure network such as the Internet.

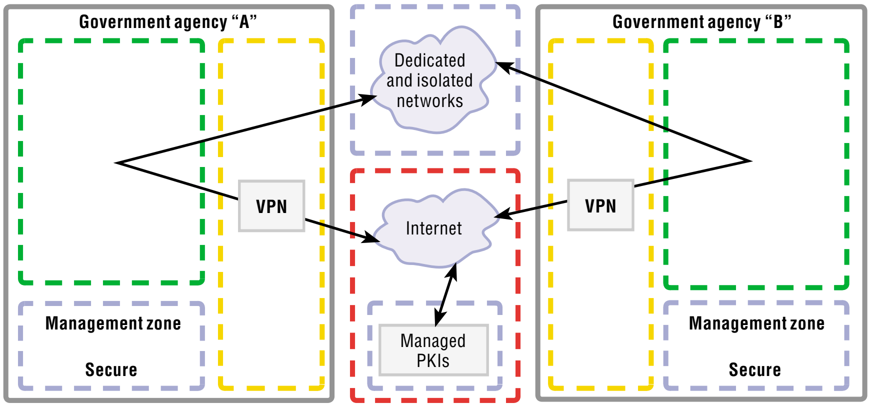

Figure 9. G2G topology.

There are multiple approaches to establishing VPNs, but a leading standards-based approach is to use the Internet Protocol, Version 6 (IPv6) IPSec packet-level confidentiality and integrity capabilities. Users can provide IPSec through software or dedicated hardware.

The G2G topology can create considerable challenges due to the large number of possible scenarios and their associated security needs. We can trifurcate the G2G space into low, medium and high requirements for assurance. An example of what might be high assurance branch would be peace-keeping coalitions. An example of what might be a medium-assurance G2G branch would be sharing clinical drug trial data between the Federal Drug Administration (FDA) and the Centers for Disease Control and Prevention (CDC). An example of a low-assurance G2G branch would be a public library system.

IBM middleware solutions for government

IBM Middleware Solutions are customized combinations of IBM core middleware and industry-specific middleware that, when combined with application software from IBM's network of independent software vendor ISV partners and industry-specific services, enable governments to build an on demand operating environment and to address the government challenges. They also help government provide highly secure access to government information, integration of data, improved compliance and increased productivity for governments and constituents. These solutions include:

- IBM Middleware Solution for Government Access. *A comprehensive suite of collaboration tools that helps provide citizens and businesses with improved, continuous and streamlined highly secure access to government information and services.*
- IBM Middleware Solution for Government On Demand Workplace. *A solution that provides government employees with simplified secure access to content, people and applications to help them deliver services to constituents more efficiently.*
- IBM Middleware Solution for Government e-Forms and Records Management. *A solution that helps government departments control document management and retention to reduce paper-based processes and redundant data entry using Web services and XML standards.*
- IBM Middleware Solution for Government Collaboration. *A solution that helps governments to achieve comprehensive horizontal collaboration and process integration across multiple lines of business. This solution can help them by connecting disparate back-end applications, enterprise software packages, legacy systems and data into a consolidated enterprise environment.*
- IBM Middleware Solution for Public Safety. *A solution that helps government emergency first responders—such as law enforcement, emergency response and transportation-management agencies—to have integrated access to geospatial data, maps and other information to facilitate better and faster decision making in emergency situations.*

The following sections combine the secure IT infrastructure topologies and interactions between entities and government to depict the security patterns for each of these solutions.

IBM Middleware Solution for Government Access (C2G)

IBM Middleware Solution for Government Access enables streamlined access to government information and allows governments to conduct online transactions for government services. Governments that are Web-enabled can use the design depicted in Figure 10 to implement the C2G, B2G1, and B2G2 entity-to-government interactions leveraging the C2G topology described on page.

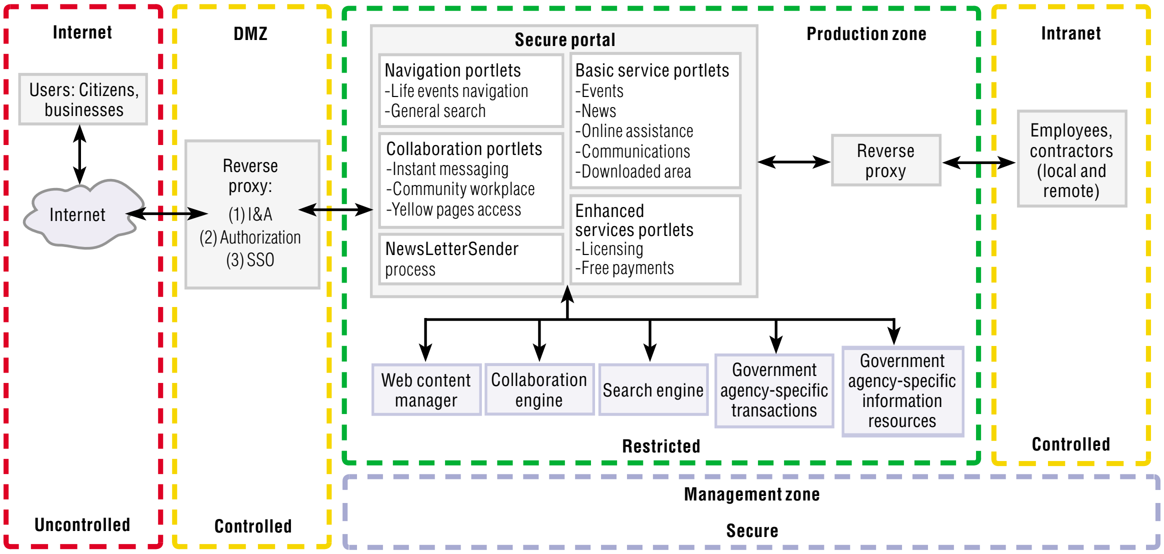

Figure 10. IBM Middleware Solution for Government Access offering components.

For governments in the initial e-government stage, this solution establishes the foundation for secure government interactions and delivers public, shared information and simple transactions through the secure portal component and management security zone. Straightforward security – such as intelligent network design, encryption, firewalls and multiple DMZs – is part of the basic construct of the portal component. For governments enhancing existing e-government services, this solution offers a secure, full-fledged, service-delivery channel to authorized providers. While governments in the initial stage provide information and make basic transactional services (such as requesting benefits) through the Internet, they can deliver more complete transactions. For example, citizens and businesses can now fill out license renewals and pay for the service using the Internet.

Naturally, citizens and businesses need to feel confident that the information and self-service features the government provides are secure. But Web-based technologies are by their nature susceptible to security threats. The outward-facing secure portal – the part that constituents see, expect and depend on – helps governments provide integrity and availability. The secure portal provides centralized security-management for authentication, authorization and auditing. With the addition of the single sign-on capability, portal users can authenticate their IDs once and receive access to integrated resources based upon their authorization and role.

The collaboration engine is an extension to the portal that can offer online instant messaging capability. The real-time collaboration afforded by this facility can provide enhanced interaction between the citizen and the government customer-relationship manager or case worker, which can lead to increased citizen satisfaction.

A key benefit of e-government is to speed service delivery while leveraging Web technologies to drive down costs. The reliability of the infrastructure helps drive better public access, decreased costs and improved efficiencies for citizens, business and governments. When e-government infrastructures become unreliable or unavailable due to slowdowns or security breaches, it affects both the customer experience and the value of undertaking the e-government initiative. Service delivery is slowed and costs might rise.

The IBM Middleware Solution for Government Access solution protects against unavailability or corruption of the information that might be caused by a security breach or destruction of information.

The solution helps government provide multiple levels of security:

- *Citizen- and business-access security only authorizes a view of their information.*
- *Online payment transactions for licenses, fees or taxes are secured end-to-end to protect the financial information as it goes from the payer through the government to the external financial service provider.*
- *Government service representatives, case workers, agents or auditors collaborate securely in real time with citizens and businesses and help them successfully complete complex online transactions.*
- *Services are protected against interruption (with back-up and restore and redundancy) with convenient one-stop, highly available (24x7), user-friendly access.*

In building a portal-based smart community with IBM Middleware solution for Government Access, government officials help improve community development. This highly secure solution can help empower citizen participation and contribution to local efforts, as well as economic, social and cultural development. Citizens have easier access to local officials, so their voices are heard. Clubs and organizations can use a secure community site and calendar to plan events around one another. Local charities, for example, can avoid holding fund-raisers on the same evening. Local students can turn to the portal to find a match for their volunteer work or review requirements for high school graduation. A secure community portal can help governments bring people together in ways that did not previously exist. For example:

- *Community centers providing health-care, education, social, human and information services can participate in the government-access portal and give citizens a single point of access to information.*
- *Municipalities can offer portal access that enables citizens to complete and submit application forms, search databases and directories, share minutes from council meetings and solicit feedback.*

IBM Middleware Solution for Government e-Forms and Records Management (C2G and B2G)

Federal, state and local governments are attempting to modernize and increase efficiency. In the U.S. the OMB has issued the implementation of the Government Paperwork Elimination Act. Despite its name, this act is not intended to totally eliminate paper, but to encourage the use of digital forms and begin the paper-to-digital transformation.

IBM Middleware Solution for Government e-Forms and Records Management provides a paperless solution to the myriad of forms required by government regulations. Governments can use this solution (see Figure 11) implements the C2G, B2G1, and B2G2 interactions between entities and the government.

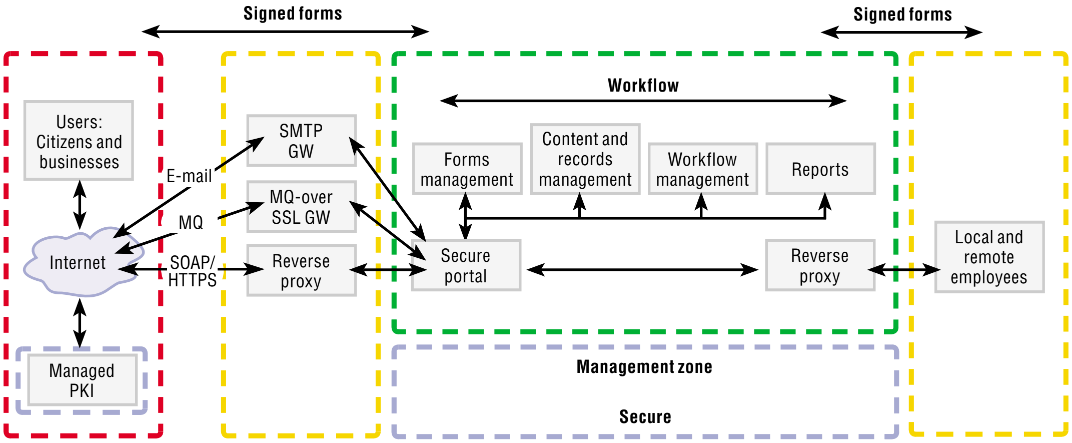

Figure 11. IBM Middleware Solution for Government e-forms and Records Management offering components.

In deploying IBM Middleware Solution for Government e-Forms and Records Management, governments can enhance their existing e-government services by offering forms over the Internet and allowing citizens and businesses to complete and submit them electronically. This solution can also be deployed on an intranet to provide self-service for benefits and life events for employees. One of the key attributes available for these forms is the ability to sign a form digitally and have it stored so that it can be trusted as a non changing record of the transaction. This level of security is vital to the movement of government forms from paper to electronic.

Security extensions to the solution can take advantage of the PKI Services to issue X.509v3 public-key digital certificates to end users who request certificate services. Certificates limit access to sensitive extranet and intranet data only to authenticated users. Certificates also enable users to digitally sign the online forms. After the digital certificates have been deployed, users can obtain certificates and even to renew or revoke them.

IBM Middleware Solution for Government On Demand Workplace

IBM Middleware Solution for Government On Demand Workplace helps enable governments to optimize their electronic interactions with their employees through intranets, e-mail and integrated workflows between existing applications and enterprise resource planning (ERP) software. It allows employees to manage personnel benefits, budgeting, accounting and other functions online. The highly secure access for this solution in Figure 12 builds upon the C2G topology.

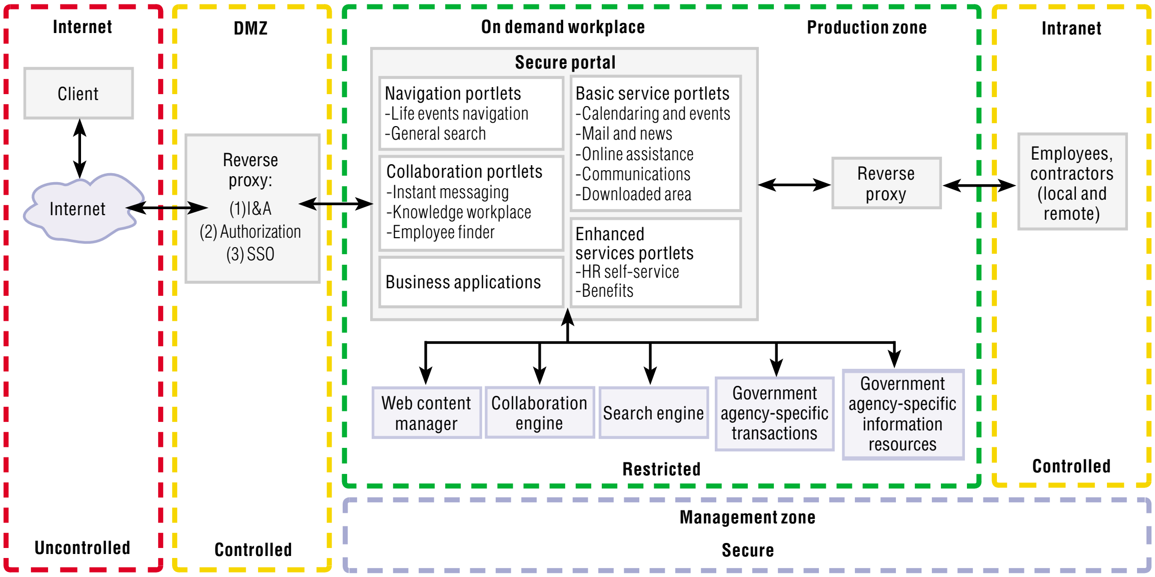

Figure 12. IBM Middleware Solution for Government On Demand Workplace offering components.

A government's workforce is fundamental to the concept of the on demand workplace. A flexible, responsive and progressive workforce initiative focused on responsiveness, productivity and knowledge is a critical component of any on demand workplace. With such a workplace, everyone becomes a knowledge worker, conducting self-service human resource responsibilities, using collaborative development and distance-learning options, and relating to each other in a new way. This workplace fosters interactive employee collaboration and information sharing with one or more experts—typically implemented through services, such as chat rooms, bulletin boards and instant messaging services. The ability to securely identify and locate employees on the network is a key to sharing information among these employees. The employee's profile, preferences and security privileges are stored on a server directory, so each client doesn't need to know the physical or direct address of other clients. It also allows the solution to implement different security levels and implement collaboration styles that include sharing applications and complex data types.

A consistent, secure portal interface integrates business systems, making it easier for employees to find and use consolidated information to support more informed decisions. Using the secure portal block shown in Figure 12, the on demand workplace provides single-sign-on security to help simplify access to applications and tools. Secure collaboration enables employees to share knowledge with each other, government agencies, partners and suppliers. Organizations can personalize a secure connection to live external news feeds to keep employees current on relevant up-to-the-minute news. The secure portal block also delivers access to personalized content and applications using role-based views, performance data, and just-in-time training and collaboration with experts.

IBM Middleware Solution for Government Collaboration

The IBM Middleware Solution for Government Collaboration provides a comprehensive government solution to help achieve secure interactions and collaborations. As shown in Figure 13, the solution links government processes and government departments by implementing the G2G1, G2G2 and G2G4 entity-to-government interactions on the G2G topology described earlier. Leveraging IBM Middleware Solution for Government Collaboration can help governments achieve business integration across multiple lines of business, integrating government processes, disparate back-end applications, enterprise software packages, legacy systems and data into a secure integrated enterprise environment.

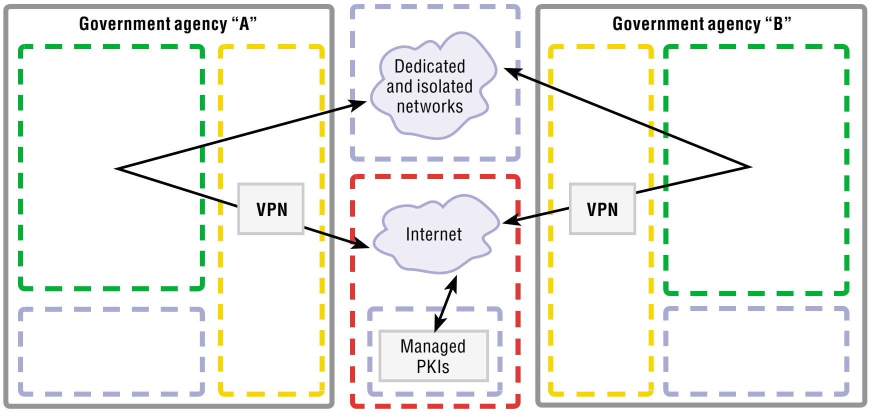

Figure 13. IBM Middleware Solution for Government Collaboration components.

In today's digital economy, constituents demand universal access to information. To satisfy this demand, many governments support multiple delivery channels including the Internet, voice recognition units, kiosks and call-center applications. Citizens expect to retrieve the same information regardless of the delivery channel they use to access the information. For example, a tax agency must ensure that citizens can retrieve tax status consistently, either through a Web site or through a voice recognition unit. At the same time, tax organizations have multiple back-end applications for property tax, business tax, withholding tax and supporting tax calculations. Because of this, many channels need to access the information from multiple back-end applications. Different delivery channels require different security levels. Call-center workers are usually allowed to see certain details about citizen accounts that aren't shown to citizens when they access their accounts. These different levels of security are tightly coupled with the requirements of the delivery channel. Because of this, the back-end application should be isolated from these details. An internal firewall is ideally suited to making these security decisions.

Also, to provide a holistic view of the citizen or business, governments need to share information and integrate processes across departments. In most cases, essential government services operate across jurisdictional boundaries. The IBM Middleware Solution for Government Collaboration solution transforms the delivery of these essential services in terms of citizen or business life cycles. This approach looks at service delivery from the service requestor's perspective and determines how jurisdictions work together securely to meet the needs of the requestor. For example, when citizens set up a business, they need to register the business at the state level, register for tax at the national level and obtain building-use permits at the local level. To let them present all these transactions as an integrated package showing a unified government means interconnecting a range of agencies as defined in the G2G topology. When a government presents a single face to the world, security becomes a significant issue. A unified government face can also involve collaboration and interconnection across departments within the same hierarchy of government. For instance, at the regional level, the welfare and tax departments' fraud processes need to be linked to enable them to pursue common violators. These and similar scenarios for providing a unified citizen view rather than a fragmented, silo-specific view require the various government departments to securely, effectively and efficiently integrate with each other.

IBM Middleware Solution for Government Collaboration helps enable governments to develop a networked infrastructure that can evolve to the "need-to-share" way of a unified government. To collaborate across government entities, this infrastructure securely integrates numerous legacy systems and data. Across this infrastructure, citizens, businesses and other government agencies share information that is sensitive and private. Securing this sensitive personal or mission-critical data requires the government to register its user so that, when the user returns, the government is certain that it is the same user. (A user ID and password, common on commercial Web sites, is no guarantee of this.) The G2G topology enables the government to authenticate the user and to establish and employ acceptable methods for the nonrepudiation of online transactions or contracts. The seven aspects of security are:

Identification. Who are you?
By browser, user to global repository, user ID or enterprise information systems (EIS)

Authentication. How do I know your identity is true?
Through Simple Object Access Protocol (SOAP), Java Messaging Service (JMS), Internet Inter-ORB Protocol (IIOP) and Java 2 Platform, Enterprise Edition (J2EE) Connector architecture (JCA)

Authorization. Are you allowed to perform this transaction?
Publishing to global repository, access catalog and EIS

Integrity. Is the data you sent the same data as the data I received?
Through SOAP, JMS, IIOP and message queuing (MQ)

Confidentiality. Are we sure that nobody read the data you sent me?
Through SOAP, JMS, IIOP, MQ and HTTPS secure sites

Auditing. Is there a record of all transactions, so we can look for security problems after the fact?
Through Web Services Gateway (WSGW)

Nonrepudiation. Can both sender and receiver provide legal proof to a third party that the sender did send the transaction, and the receiver received the identical transaction?
Through WSGW

IBM Middleware Solution for Public Safety

IBM Middleware Solution for Public Safety enables organizations inside and outside of government to retrieve certain critical data to take coordinated action. These actions may be to facilitate crime prevention, disease control, or to react to a disaster. IBM Middleware Solution for Public Safety implements the G2G1, G2G2, G2G3, G2G4, and G2G5 entity-government interactions on the G2G or B2G topologies described earlier. Organizations can leverage the G2G topology as shown in Figure 14 to secure this solution when deployed across government entities. They can also use the B2G topology as shown in Figure 15 to secure this solution when deployed between government and hospitals or other non government public safety organizations. Regardless, the focus is on improving communications and coordination among first-responder agencies—defined as members of law enforcement, fire, other public safety, transportation and public health agencies that respond to emergency events.

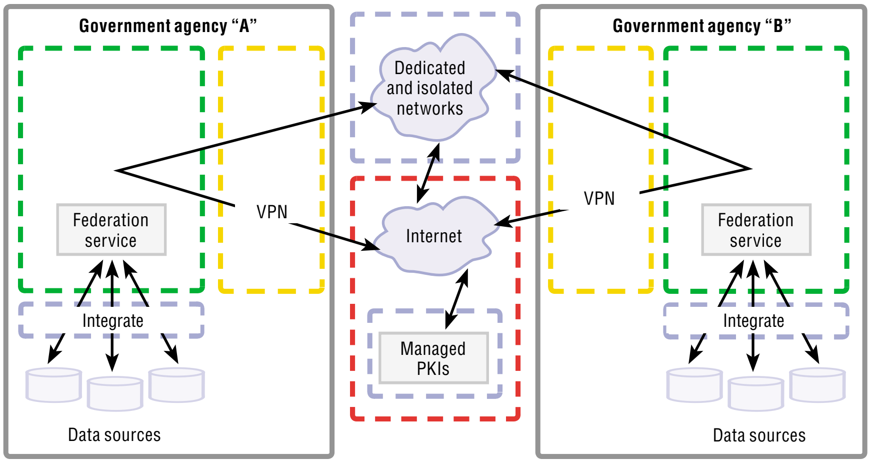

Figure 14. G2G public safety components.

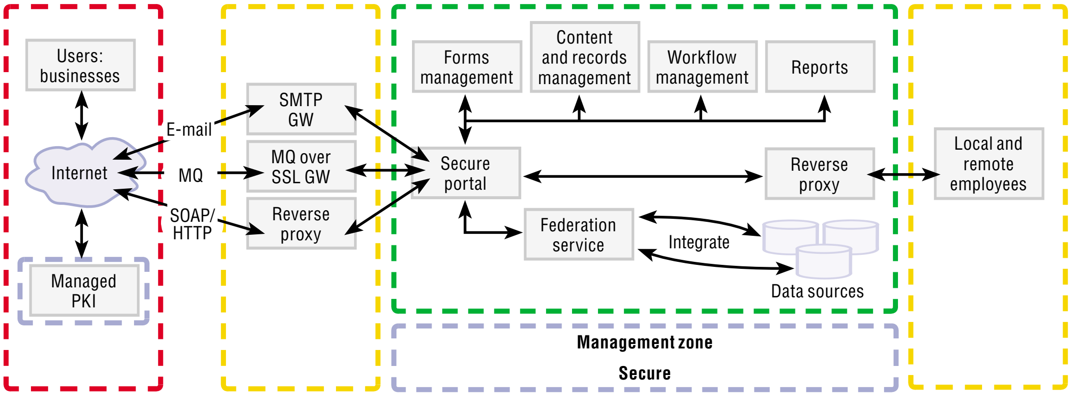

Figure 15. G2B public safety components.

Dual use and vertical and horizontal information sharing are two important public safety security factors. Dual use is the concept of leveraging public safety security investments for multiple uses. Vertical and horizontal information sharing is the concept of optimizing the secure sharing of information between federal, state and local agencies (and other organizations as appropriate). IBM Middleware Solution for Public Safety helps protect valuable or classified information, helps guard the cooperating organizations' IT infrastructures and helps securely enable vertical and horizontal information sharing. This allows governments to shift from "need to know" to "need to share" by making information available in a highly secure environment when it is needed for the safety and protection of the public.

The federation component of IBM Middleware Solution for Public Safety securely integrates scattered and heterogeneous data. Federated search capabilities provide integrated, real-time access to diverse data – as if it were a single database, regardless of where it resides. This component allows users to integrate diverse, distributed data without moving it. It results in a complete view of timely information – anytime, anywhere. Securing levels of authorized access to this federated information is critical so government organizations and external public safety organizations can:

- *Make informed decisions.*
- *Assess current risks.*
- *Protect against attacks, natural disasters and other incidents.*
- *Detect potential threats.*
- *Recover from harmful incidents.*

Internal users, including first responders, incident managers and situational analysts, need authorization to access classified data integrated from many sources. First responders can use a highly secure extranet connection to access this data remotely. Transmitted information can be encrypted to protect it from unauthorized viewing. Governors, mayors or other elected officials have access to information to help them make announcements and judgments for their immediate constituency.

External users, such as the Red Cross, emergency care teams and hospitals, have access only to data related to local conditions and information required to provide optimal health care. These external users connect to this data using the Internet.

Coordinated incident management by first-responder agencies is the fundamental business need addressed by this solution. Currently, first responders find it difficult to coordinate with each other because of five issues that must be addressed to improve the interoperability of public safety and transportation communication systems.

- *Coordination and partnerships*
- *Funding*
- *Spectrum*
- *Standards and technology*
- *Security*

Any mission-critical information system, especially when it involves wireless components, raises legitimate security questions. The solution incorporates Two-Party Key Distribution Protocol (2PKDP) security technology that combines bidirectional authentication with secure-key distribution. This robust solution also provides Data Encryption Standard (DES), Federal Information Processing Standard (FIPS) 46-3 or RC5 encryption and decryption algorithms for traffic in and out of the Web application server.

IBM Middleware Solution for Public Safety also provides a framework for a secure mobile-messaging network to disseminate critical-incident information to all first-responder teams. This framework provides security for synchronization and exchange of information among authenticated, designated parties. Team members are able to link with legacy systems from other first-responder agencies, command centers, and state and local governments – thus facilitating data federation and information sharing.

Current security offerings used in government solutions

Security and privacy components are provided by IBM Tivoli® solutions. The general approach is to keep security and privacy logic out of applications – to provide security through standard environments, protocols and application programming interfaces (APIs), such as Web services, J2EE, Java Authentication and Authorization Services (JAAS), Authorization API (aznAPI), Java Authorization Contract for Containers (JACC) and others.

IBM Tivoli security management middleware solutions address critical security challenges for government organizations, in part using automated identity management and security-event management to help provide a secure on demand infrastructure. This infrastructure can meet critical and evolving government requirements for open-standards-based business integration. IBM is an industry leader in open Web services and Java security infrastructure. IBM strongly advocates open standards that address interoperability, working with key industry security players such as VeriSign and Cisco and interoperating with other solutions, such as Microsoft® .NET.

Many governments' acquisition policies now require them to buy products that have undergone formal security evaluations. IBM has achieved U.S. Common Criteria Certification on many middleware and security products (including IBM Tivoli Access Manager for e-business, Version 4.16) and is aggressively pursuing security evaluations (such as the Common Criteria and the Cryptographic Module Validation Program) for its products. For the latest status of completed and in-progress security evaluations, visit:

ibm.com/security/standards/st_evaluations.shtml

IBM Middleware for Security, Privacy, Identity, Events and Compliance

Figure 16 shows an overview of the IBM Tivoli security components within their respective topology zones. These components interoperate and integrate with each other, and are increasingly used as the standard security technology by other IBM products, including IBM WebSphere® Application Server, IBM WebSphere Portal and IBM Lotus® Workplace.

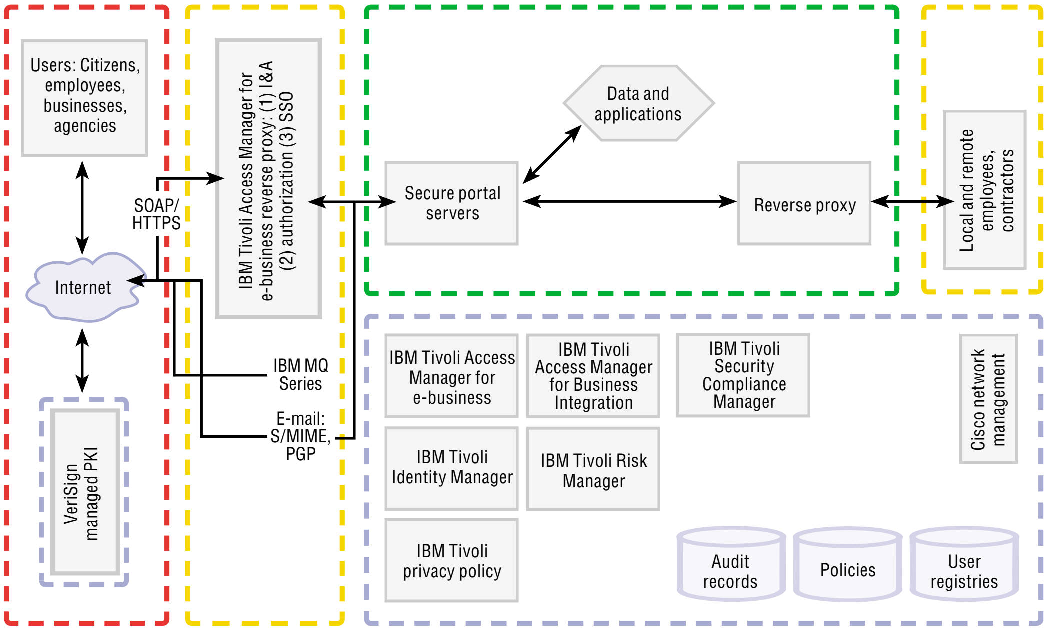
Users: Citizens, employees, businesses, agencies
SOAP/ HTTPS
Internet
VeriSign managed PKI
IBM Tivoli Access Manager for e-business reverse proxy: (1) I&A (2) authorization (3) SSO
IBM MQ Series
E-mail: S/MIME, PGP
Data and applications
Secure portal servers
Reverse proxy
Local and remote employees, contractors
IBM Tivoli Access Manager for e-business
IBM Tivoli Access Manager for Business Integration
IBM Tivoli Security Compliance Manager
Cisco network management
IBM Tivoli Identity Manager
IBM Tivoli Risk Manager
IBM Tivoli privacy policy
Audit records
Policies
User registries

Figure 16. Tivoli secret overview

IBM Tivoli Access Manager for e-business[7]

Tivoli Access Manager for e-business is an access-control solution for on demand business applications. Tivoli Access Manager for e-business integrates with on demand business applications to help deliver a secure, unified and personalized on demand business experience. By providing standards-based authentication and authorization APIs and integration with application platforms, such as J2EE and Microsoft .NET, Tivoli Access Manager for e-business helps secure access to critical applications and data spread across the extended enterprise.

Web-based single sign-on can span multiple sites or domains by exploiting Tivoli Access Manager for e-business cross-domain single sign-on technology or by using Security Assurance Markup Language (SAML) and other token-passing protocols.

Tivoli Access Manager for e-business reverse proxy

The Tivoli Access Manager for e-business reverse proxy provides the authentication mechanisms used in the I&A process to protect access to a Web environment and provide Web-based single sign-on. Mechanisms supported include:

- *Passwd/LDAP: Password authentication (Forms/BasicAuth)*
- *Token-Cdas: Token authentication*
- *cert-ldap: SSLv3 and TLS client certificate authentication*
- *http-request: HTTP header authentication*
- *CDSSO: electronic community single sign-on*
  Note: This will be deprecated when support for Web Services is available.

A general-purpose exit, Cross-Domain Authentication Service (CDAS), enables authentication mechanisms to be added to Tivoli Access Manager. CDAS is used to integrate Daon's biometric authentication framework with Tivoli Access Manager to support biometric-based authentication. Tivoli Access Manager also supports step-up authentication policies where already-authenticated users request access to a resource with a higher sensitivity. Tivoli Access Manager supports multifactor authentication.

Integrating IBM Tivoli security solutions and VeriSign Unified Authentication Services

VeriSign Unified Authentication Service (UAS) extends the VeriSign Managed PKI (MPKI) solution and can support multiple means of authentication—including dynamic one-time passwords (OTP), token-generated PKI and desktop PKI—on a single platform. Designed to radically reduce the hidden costs of administration and maintenance for an enterprise, VeriSign Unified Authentication Service minimizes new infrastructure requirements and leverages VeriSign's service infrastructure to enable provisioning and validation of authentication credentials. The solution is built on known, open standards such as X.509, RADIUS, LDAP and open database connectivity (ODBC), allowing for easy integration into an existing identity-management environment. Figure 17 shows the high-level deployment architecture for VeriSign UAS in an IBM Tivoli environment. A range of components are included.

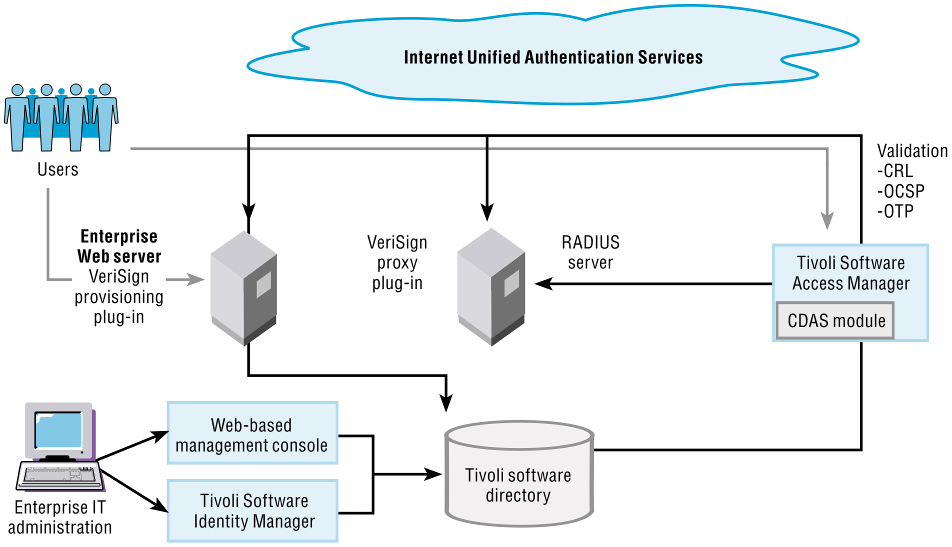
Internet Unified Authentication Services
Users
Validation
-CRL
-OCSP
-OTP
Enterprise Web server
VeriSign provisioning plug-in
VeriSign proxy plug-in
RADIUS server
Tivoli Software Access Manager
CDAS module
Web-based management console
Tivoli Software Identity Manager
Tivoli software directory
Enterprise IT administration

Figure 17. IBM Tivoli-VeriSign UAS Architecture.

Next-generation token

VeriSign secure token is an all-in-one security token capable of both OTP and PKI authentication. OTP authentication doesn't require client software to be deployed on the user desktop. In fact, the device has a small LCD display for showing the OTP to the user and a button to trigger the next OTP value. The OTP algorithm is sequence-based. This device is also capable of supporting PKI authentication, digital signature and encryption in the plugged-in mode. For certificate operations, the token has a Universal Serial Bus (USB) connector and embeds a smart card chip.

No-new-infrastructure deployment model

The VeriSign solution doesn't require users to deploy a new infrastructure. In fact, the solution uses existing identity-management components – directories such as LDAP stores and AAA infrastructure such as RADIUS servers. Using a hybrid token that supports multiple means of authentication (as shown in Figure 18), users can deploy the UAS solution on top of the existing Tivoli directory infrastructure. This approach consolidates all management and administration functions on the LDAP server, effectively making the directory the command-and-control center across all systems.

Flexible integration components

For in-premise integration, VeriSign UAS leverages lightweight integration software. This software comprises a small but flexible set of software components. For credential provisioning and OTP validation, VeriSign provides a lightweight stateless provisioning server, called Provisioning Proxy and RADIUS proxy server. This unique combination of in-premise software and VeriSign-managed services reduces the hidden costs of administration and maintenance for government agencies. It is also extremely easy to use – helping to address traditional impediments to strong authentication deployment.

Figure 18. Secure token capable of OTP and PKI authentication.

Tivoli Access Manager CDAS plug-in

The VeriSign UAS solution includes a CDAS plug-in for the Tivoli Access Manager reverse proxy. This CDAS plug-in enables certificate- and token-based authentication in a Tivoli Access Manager deployment. The CDAS plug-in supports PKI validation, using Certificate Revocation Lists (CRLs) or Open Certificate Status Protocol (OCSP) and OTP validation.

Also, to create custom authentication modules, VeriSign can provide a complete integration software development kit (SDK) for C and Java code. The SDK can be used by the VeriSign or IBM professional services team to create custom-validation modules, which can be used across specific terminal-server systems and servers when these systems do not have built-in PKI or RADIUS validation capabilities.

Control inside—complexity of security, reliability and scale outside

With the VeriSign solution, a government agency always remains in control of all identity management data and policies. All user identities, credential templates and authorization policies remain within the government agency directory under the strict supervision and control of the agency. Complexity is dramatically reduced by moving all critical security components to the VeriSign network. The same infrastructure that provides e-commerce to the whole Internet ensures 7x24x365 access and high availability to the customer.

Certificate and OTP validation are performed in the VeriSign domain. To ensure maximal reliability, redundancy and failover, VeriSign deploys OTP validation on top of its DNS infrastructure, the Advanced Transaction Lookup and Signaling system (ATLAS). This infrastructure resolves 10 billion* or 1010 Domain Name Server (DNS) queries every day. The ATLAS infrastructure comprises 13 data-centers distributed around the world. Thus, VeriSign UAS mirrors the IBM standards for security expertise, superb technology platforms, and operational excellence.

Self-service applications

VeriSign Unified Authentication Service can help reduce high authentication costs by providing token end users with self-service capabilities across the life cycle of the device. The VeriSign UAS also provides built-in self-service applications for:

- *Certificate enrollment and renewal*
- *Token registration and activation*
- *Lost and broken tokens*
- *Lost PIN and PIN resets*
- *Out-of-sync and locked tokens*

Users can do this with the VeriSign UAS self-service console or through IBM Tivoli Identity Manager. VeriSign UAS also supports complete administrator and helpdesk functionalities – both natively and through Tivoli Identity Manager.

Integrating Tivoli Access Manager with IBM WebSphere Portal [8]

WebSphere Application Server security includes its own services for authentication and authorization, which are available only to WebSphere applications. WebSphere Portal is an application running on WebSphere Application Server that can use the WebSphere Application Server's security services. IBM Tivoli Access Manager for e-business enables organizations to consistently enforce their security policies across WebSphere and other applications. The recommended approach is for a single, unified security model, using IBM Tivoli Access Manager for e-business to provide the security infrastructure. IBM Tivoli Access Manager for e-business manages the access to all WebSphere Portal resources, thus providing a single security model.

IBM Tivoli Access Manager for Business Integration [9]

IBM Tivoli Access Manager for Business Integration is a multiplatform security-management solution that upgrades the native security services of IBM WebSphere MQ to those provided by IBM WebSphere MQ Extended Security Edition. IBM Tivoli Access Manager for Business Integration provides application-level data protection for WebSphere MQ software-based applications without modifying or recompiling them.

Application-level data protection differs from link-level or channel-level data protection in that the integrity and confidentiality of messages can be demonstrated, not only while messages are in transit from system to system, but also while they are under the control of WebSphere MQ—that is, resident in a queue. This can be critical for organizations using WebSphere MQ to process personally identifiable information or other types of sensitive data, such as high-value financial transactions.

IBM Tivoli Security Compliance Manager [10]

IBM Tivoli Security Compliance Manager can act as an early-warning system by identifying security vulnerabilities and security policy. Tivoli Security Compliance Manager helps organizations of all sizes define consistent security policies and monitor compliance with these defined security policies—whether the policies are based on internal security requirements, industry-standard security policies or both.

IBM Tivoli Identity Manager[11]

To compete effectively in today's IT environment, organizations are increasing the number of users – customers, employees, business partners and suppliers – allowed to access information. As IT is challenged to do more with fewer resources, it is increasingly important to effectively manage user identities throughout their life cycles. IBM Tivoli Identity Manager can provide a secure, automated and policy-based user-management solution that helps address these key business issues across both legacy and on demand business environments. Intuitive Web administrative and self-service interfaces integrate with existing business processes to help simplify and automate managing and provisioning users. The solution incorporates a workflow engine and leverages identity data for activities such as audit and reporting.

IBM Tivoli Risk Manager[12]

Tivoli Risk Manager helps organizations centrally manage security incidents from a single Web-based security console. Organizations can leverage this communications and control center to assess enterprise vulnerabilities – help them detect and assess attacks, threats and exposures. Tivoli Risk Manager does this by correlating security information and risk alerts from firewalls, routers, networks, host- and application-based intrusion detection systems, desktops, and vulnerability-scanning tools. The centralized console provides real-time visualization and management of security incidents.

Tivoli Risk Manager software now includes IBM Tivoli Enterprise Console® and IBM Tivoli NetView® to deliver a solid event-correlation solution. Integration between Tivoli Enterprise Console and Tivoli NetView allows users to examine the network topology to see where the affected resources are located – delivering root-cause problem determination. Users can also drill up from the network console to determine other resources that might be affected as a result of a network outage. And when combined with IBM Tivoli Business Systems Manager and IBM Tivoli Service Level Advisor, users can deploy a powerful solution capable of managing both system and network resources as well as business processes.

Tivoli Risk Manager also includes the Tivoli Data Warehouse. Tivoli Risk Manager lets organizations store security events in the data warehouse for long-term persistence. With Tivoli Data Warehouse, they can also store events from other sources, such as configuration and monitoring. New data warehouse reporting capabilities can be used to leverage the information.

Tivoli Risk Manager helps deliver on the autonomic computing tenets of self-configuration and self-protection by assessing potential security threats and automating responses, such as server reconfiguration, security patch deployment and account revocation. Tivoli Risk Manager also produces periodic heartbeats used by upstream servers to help verify that specific systems are still operational. It delivers self-configuring autonomic computing capabilities by assessing potential security vulnerabilities and responding with actions, such as server reconfiguration or security-patch deployment. This helps businesses to minimize risk and business exposure, and in some instances, restore the business to its original secure state without manual intervention.

IBM Tivoli Privacy Manager for e-business[13]

Within the next decade, experts expect data warehousing on the petabyte (1000-terabyte) scale to be commonplace, with much of that data being sensitive personally identifiable information about customers, business partners and employees. This trend creates a significant management challenge, especially as privacy and data protection laws and regulations place new restrictions on the use of personally identifiable information, and consumers and governments increasingly demand control over how others may use their personal data. Many organizations face significant exposure in their data-handling practices — exposure that manually managed policies cannot mitigate.

IBM Tivoli Privacy Manager for e-business is an enterprise privacy-management solution designed to address these challenges by providing middleware to abstract privacy and data-handling rules from applications and IT systems. With this approach, privacy-sensitive data is linked to policy at the point of collection, and subsequent requests to use the data are then filtered, permitted or denied according to policy and the data owner’s preferences. Users can also generate audit trails of data usage automatically. Tivoli Privacy Manager for e-business enables organizations to automate the management of personal information and help cut the costs of privacy management and mitigate the risks of unauthorized disclosure.

Tivoli Privacy Manager for e-business contains software components that allow your organization to:

- *Centralize the authorship and management of your privacy rules.*
- *Deploy policy across monitored applications and IT systems automatically.*
- *Respect privacy decisions of individuals across monitored systems.*
- *Deploy initiatives faster by eliminating the need to code privacy rules into applications.*
- *Assess compliance to policy by automatically generating audit reports.*

IBM Tivoli Provisioning Manager, IBM Tivoli Configuration Manager and IBM Tivoli Intelligent ThinkDynamic Orchestrator

Tivoli Provisioning Manager[14] helps ensure availability of systems by enabling on demand computing across the data center through server, storage and network automation. Tivoli Provisioning Manager, through workflows, can automate the manual provisioning and deployment process. It uses prebuilt workflows to control and configure major vendors' products. Users can also create customized or modify the prebuilt workflows to implement their organization's data-center best practices and procedures. They can then automate and run these procedures consistently and with virtually no error.

Tivoli Provisioning Manager comes with a predefined set of workflows supporting products from IBM, Cisco, Sun, VMware, Citrix, Siebel and Microsoft. These workflows can automate unique data center processes including the installation, configuration and deployment of servers, operating systems, middleware, applications, storage and network devices. When a new server is provisioned, IBM Tivoli Provisioning Manager can deploy and configure the IBM Tivoli Management Agent across a network of servers. Workflows are provided with the product to enable integration of IBM Tivoli Provisioning Manager software install capability with robust IBM Tivoli Configuration Manager software-distribution capabilities to enable a complete installation from operating system to application. Users can also install software updates and security patches to keep configurations current and help limit exposure to known threats. IBM Tivoli Provisioning Manager is also tightly integrated with IBM Tivoli Intelligent ThinkDynamic Orchestrator,[15] allowing users to run automated tasks in response to or in anticipation of changing conditions, creating an automated on demand environment.

IBM Tivoli Directory Server[16]

IBM Tivoli Directory Server provides a powerful, standards-conformant LDAP identity infrastructure that is the foundation for deploying comprehensive identity management applications and advanced software architectures such as Web services.

Operating systems[17]

IBM has a long history of providing robust, secure operating systems. The current set of IBM operating systems that are suitable for deployment as part of a government security solution include:

- *IBM z/OS®*
- *IBM AIX®*
- *IBM z/VM®*
- *IBM OS/400®*

IBM also partners with makers of the leading Linux® distributions for all its IBM @server® platforms. IBM middleware products also run on Microsoft Windows® and other vendors' UNIX® offerings.

IBM Tivoli Access Manager for Operating Systems

IBM extends security to a wide range of operating systems with an easy-to-use, robust security system. IBM Tivoli Access Manager for Operating Systems securely locks down business-critical applications, files and operating platforms to help prevent unauthorized access. This security capability can block both insiders and outsiders from unauthorized access to valuable customer, employee and business partner data. Tivoli Access Manager for Operating Systems also audits application and platform activity. This capability helps provide the assurance that customers, employees and partners expect—and the rigorous auditing that the government and senior management require.

Integration with IBM Tivoli Identity Manager extends UNIX and Linux user management by allowing UNIX and Linux identities, passwords and permissions to be managed along with those of other platforms and directories. These platforms and directories include Microsoft Windows, IBM AS/400®, IBM @server® iSeries™ and the IBM OS/390® Security Server for Resource Access Control Facility (IBM RACF®).

VeriSign authentication services and solutions

The VeriSign Managed PKI (MPKI) offering uses a VeriSign back-end provisioning and life-cycle management platform for PKI credentials and includes an in-premise registry authority for enterprise enrollment. A Web application can be hosted either by the enterprise or by VeriSign to provide administrative and user-management functionality. It contains support for most LDAP directories including IBM Tivoli Directory Server, ODBC and various server platforms.

VeriSign authentication services and solutions include the following:

- *VeriSign Managed PKI Service for the Federal Bridge Certification Authority allows government agencies to have a fully operational, Federal Bridge Certification Authority (FBCA)-compliant PKI up and running quickly.*
- *VeriSign Interim External Certificate Authority (IECA) Digital Certificates allows the Department of Defense and its contractors to securely access department Web sites, exchange secure mail with the Department of Defense and digitally sign documents and electronic forms.*
- *VeriSign Unified Authentication Service as detailed above extends the MPKI platform by offering additional modules to support OTP credentials. It is a single platform for issuing and managing multiple credential types including certificates, tokens and OTP devices*
- *VeriSign Consumer and Business Authentication Services deliver on VeriSign's reputation as a proven industry leader that has pioneered industry practices for authenticating individuals and businesses. As part of its SSL issuance process, VeriSign authenticates over 400 000 businesses every year. Using VeriSign authentication services, businesses and individuals can authenticate and conduct transactions with confidence.*
- *VeriSign Strong Authentication solutions, including Managed PKI to provide PKI and digital signatures allows The General Services Administration Access Certificates for Electronic Services (ACES) Program to provide data confidentiality, data integrity, user authentication and user nonrepudiation for C2G and B2G transactions.*

IBM Secure Identity Solution for e-business

Many people have access to multiple applications, each with its own user management and password management, so they're challenged with remembering several user name and password combinations. This causes problems for both users and administrators. For example:

- *In an attempt to remember their login information, users employ the same user name and password combination as often as possible, writing the user name and password on paper or storing it in a text file. The security risk is obvious.*
- *Administrators face more work to ensure that users are added to or removed from the proper database as needed. Manually adding and deactivating accounts is typically time-consuming and subject to error.*

The solution to the first problem is single sign-on. The solution to the second is identity management. However, different access-control applications require different level of authentication. Complying with all applications' authentication requirements means a flexible single sign-on solution that can perform multifactor authentication based on one or any combination of information a user knows, an item or thing in his or her possession and his or her identity. Single sign-on combined with automated identity management is a robust solution that enhances security and reduces the cost of access-control management.

IBM has recognized these issues – common to many organizations – and has worked with IBM Business Partners, such as GE Security and ActivCard, to develop a secure identity solution, based on issuing a Smart Card to each individual. The Smart Card can securely store the user name and password of several applications or provide a pointer to the data on a secure server. It can also store a biometrics and a digital certificate. This IBM solution for card issuance and management can be used for physical and logical access control. Figure 19 shows the architecture of the IBM solution.

The components of the solution are:

- *Tivoli Identity Manager provides automated user provisioning and deprovisioning. It also handles application password management.*
- *The Physical Access Control System (GE in Figure 19) provides physical access control and card issuance for both logical and physical access.*
- *ActivCard software provides single sign-on for logical access control. It also communicates with Tivoli Identity Manager for password management and with GE Picture Perfect for card issuance.*
- *VeriSign PKI Services provides digital-certificate issuance and management.*

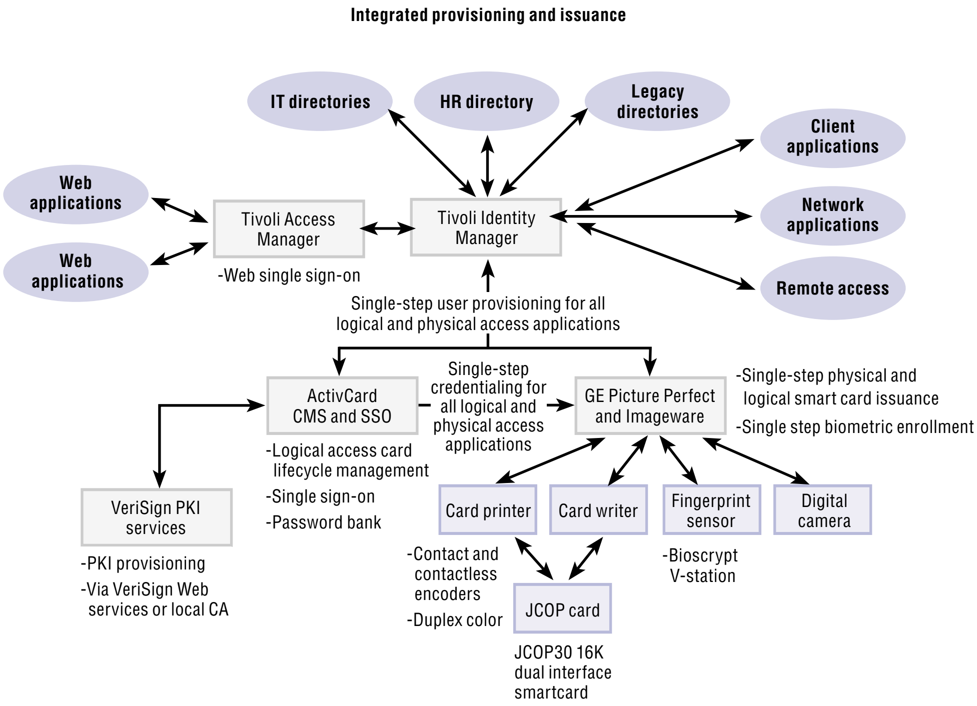
Integrated provisioning and issuance
IT directories
HR directory
Legacy directories
Client applications
Web applications
Web applications
Tivoli Access Manager
Tivoli Identity Manager
Network applications
-Web single sign-on
Remote access
Single-step user provisioning for all logical and physical access applications
ActivCard CMS and SSO
Single-step credentialing for all logical and physical access applications
GE Picture Perfect and Imageware
-Single-step physical and logical smart card issuance
-Single step biometric enrollment
-Logical access card lifecycle management
-Single sign-on
-Password bank
VeriSign PKI services
Card printer
Card writer
Fingerprint sensor
Digital camera
-PKI provisioning
-Via VeriSign Web services or local CA
-Contact and contactless encoders
-Duplex color
JCOP card
-Bioscrypt V-station
JCOP30 16K dual interface smartcard

Figure 19. IBM secure identity components.

IBM and Cisco Systems Enterprise security

IBM and Cisco Systems have collaborated on a new model for enterprise security designed to help organizations tackle their top security challenges and reduce costs. This collaboration integrates their products and creates an integrated security architecture that spans many critical points of computing—from laptops to headquarters data. This standards-based approach can help simplify security, reduce implementation and administration costs and bolster productivity.

The current set of IBM-Cisco security offerings[18] include:

- *Integrated user provisioning*
- *Integrated endpoint security*
- *Automated compliance*
- *Security services*

IBM and VeriSign integrate security for government

IBM, with its worldwide network of consultants and business partners, helps government organizations integrate business processes from end to end. Across organizations and at all levels of government—globally or locally—IBM can enable e-government for the on demand era. VeriSign, a leading provider of Intelligence and Control Services, offers comprehensive critical infrastructure and solutions, helping to ensure that government can provide secure mission-critical commerce, communication and collaboration. The IBM solutions and VeriSign services complement each other to help government agencies to:

- *Develop, implement, integrate and manage comprehensive, secure-identity solutions for complex environments.*
- *Provide security and critical infrastructure services for networks that hold critical or sensitive information.*
- *Allow e-governments to provide access control, authentication, encryption, and digital signature or e-form services to customers.*
- *Enable collaboration across government to quickly address safety threats and concerns.*
- *Enhance safety and security with state-of-the-art identity verification technologies.*
- *Facilitate the secure verification of authorized and approved individuals.*

As part of a global security alliance, IBM and VeriSign help enable the delivery of integrated secure solutions today and leading-edge collaboration in emerging technologies and security standards. The alliance enables industry-leading identity, authentication and authorization solutions by combining highly secure infrastructure capabilities and authentication services from VeriSign with security products and professional services from IBM. Well-integrated business processes and infrastructure can help e-governments work more efficiently, effectively and securely. IBM and VeriSign have the experience and the know-how to enable on demand e-government.

Examples of security products and services for government agencies include:

- *IBM Tivoli Access Manager*
- *IBM Tivoli Identity Manager*
- *IBM Secure Identity Solution for e-business*
- *VeriSign Managed PKI Service for the Federal Bridge Certification Authority*
- *VeriSign Strong Authentication solutions.*
- *VeriSign IECA Digital Certificates*
- *VeriSign Strong Authentication Services*

Why IBM?

IBM is a solid choice to help governments with secure access, because it is:

- *Highly experienced in developing, implementing, integrating and managing comprehensive secure identity solutions for complex environments.*
- *A provider of highly effective security software, hardware, services and technology.*
- *Equipped with consulting, project management and training capabilities that are key to security projects.*
- *Experienced with enterprise architectures and change-management processes.*

Why VeriSign?

As an IBM Business Partner, VeriSign can:

- *Deliver critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure.*
- *Provide strong authentication services, to leverage its global infrastructure and help ensure security.*
- *Share expertise in enabling the security of networks that hold key or sensitive information through 24X7 management of the network security infrastructure to detect, prevent, and respond to network attacks, intrusions and other system failures.*
- *Use its experience application security, enabling e-government to provide access control, authentication, encryption, and digital signature or e-form services to customers.*

VeriSign offers government agencies a comprehensive and cost-effective solution that meets FBCA and Department of Defense technical interoperability requirements for PKI-based security. VeriSign Managed PKI Service lets federal, state and local government agencies implement a PKI and Certificate Authority (CA) quickly, without the expense of designing, building, staffing and maintaining an in-house PKI platform.

Next steps

IBM, working with VeriSign and key Business Partners, provides solutions and services to help government organizations securely automate and manage key government processes. We can provide architectural and end-to-end solutions for security and services to help you achieve an on demand government.

Complementary IBM and VeriSign solutions can support your government-security efforts by providing:

- *Technical presentations and demonstrations on secure government solutions*
- *Assessment workshop and review of outcomes*
- *Proof-of-concept development for government solutions*
- *Pilot project development and implementation*
- *Full-scope project development and implementation*

For more information

To learn more about the IBM solutions for government or to access case studies and more detailed information about solution components, visit:

ibm.com/software/industries/govt

To learn more about how to improve secure information access for citizens, business and cross-government with digital credentials, digital signature, strong authentication, access and identity management, visit:

ibm.com/software/tivoli/solutions/security/

ibm.com/software/alliances/verisign

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
08-04
All Rights Reserved

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect its business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its products or services ensure compliance with any law or regulation.

Software products and services provided by third parties are sold or licensed under the terms and conditions of the third-party providers. Product availability, warranty services and support for third-party products are the direct responsibility of the third-party providers. IBM is not liable for and makes no representations, warranties or guarantees regarding third-party products or services.

The related Web address section of this publication provides addresses to non-IBM Web sites. IBM is not responsible for the content on such sites.

[1] Visit www.fedcirc.gov/library/legislation/FISMA.html.

[2] For details, visit ibm.com/security/patterns/whpapers.shtml.

[3] A risk exists that organizations might incorrectly place sensitive (that is, nonpublic) data onto these Web servers. You can use IBM technology, in conjunction with best-practice processes, to validate the data before publishing it to the Internet.

[4] Insecure communication channels, such as unencrypted e-mail, are not discussed, because this is out of policy for G2G.

[5] Visit www.ietf.org/rfc/rfc2401.txt.

[6] IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5 was evaluated under the Common Criteria at Evaluated Assurance Level 3 (Augmented) for IBM AIX, Version 5.2, SuSE Linux Enterprise Server, Version 8, Microsoft Windows 2000 Advanced Server SP3 and Sun Solaris operating environment, Version 8. The certification report was published on 16 October 2003. IBM Tivoli Identity Manager, Version 4.5.1 is in evaluation under the Common Criteria with a conformance claim of EAL3. IBM DB2 Universal Database™ for Linux, UNIX and Windows, Version 8.1 - Personal Edition, Workgroup Edition, Enterprise Server Edition and Express Edition is in evaluation under the Common Criteria with a conformance claim of EAL4 Augmented. IBM DB2® Content Manager for Multiplatforms, Version 8.2 is in evaluation under the Common Criteria with a conformance claim of EAL3 Augmented. WebSphere Application Server, Version 5.0.2 is in evaluation under the Common Criteria with a conformance claim of EAL2 Augmented. WebSphere Portal, Version 5.0.2 is in evaluation under the Common Criteria with a conformance claim of EAL2. WebSphere MQ, Version 5.3 is in evaluation under the Common Criteria with a conformance claim of EAL2.

[7] For more details, visit **ibm.com**/software/tivoli/products/access-mgr-e-bus/.

[8] For more details, visit www.devx.com/ibm/Article/16034/0/page/1.

[9] For more details, visit **ibm.com**/software/tivoli/products/access-mgr-bus-integration/.

[10] For more information, visit **ibm.com**/software/tivoli/products/security-compliance-mgr/.

[11] For more information, visit **ibm.com**/software/tivoli/products/identity-mgr/.

[12] For more information, visit **ibm.com**/software/tivoli/products/risk-mgr/.

[13] For details, visit **ibm.com**/software/tivoli/products/privacy-mgr-e-bus/.

[14] For details, visit **ibm.com**/software/tivoli/products/prov-mgr/.

[15] For details, visit: **ibm.com**/software/tivoli/products/intell-orch/.

[16] For details, visit **ibm.com**/software/tivoli/products/directory-server/.

[17] For details, visit **ibm.com**/content/home/store_IBMPublicUSA/en_US/eServer/eServer.html and **ibm.com**/security/products/index.shtml.

[18] For more detail, visit ftp://ftp.software.**ibm.com**/software/tivoli/whitepapers/wp-security-providers.pdf.

[*] "Billion" refers to the U.S. value (1 000 000 000) and not the British value.