Identity Services Infrastructure™

A practical approach to ensuring trust and privacy in government and industry

CORESTREET SOLUTIONS | WHITEPAPER

Identity Services Infrastructure

A practical approach to ensuring trust and privacy in government and industry

In the first part of the 21st century the critical enabling infrastructure will be identity services.

In the past, the walls of a village, potable and irrigable water, along with cheap and widely available power and communications, were common public goods that enabled societies to advance. Now, reliable identity services will underlie the success of modern societies. Cities and countries with modern economies will find that ubiquitous, efficient, and easy identity assurance technologies provide them with competitive advantages. Conversely, economies that lack this fundamental identity management capability will be hindered just as if they lacked a modern physical infrastructure.

The most successful communities will be those that enable individuals and organizations, both public and private, to manage a wide range of transactions easily. This will be done through Identity Services Infrastructure (ISI). This new infrastructure enables a lifestyle, efficiency, and a level of economic well-being far in advance of that provided by communities without ISI.

Societal advances and infrastructure

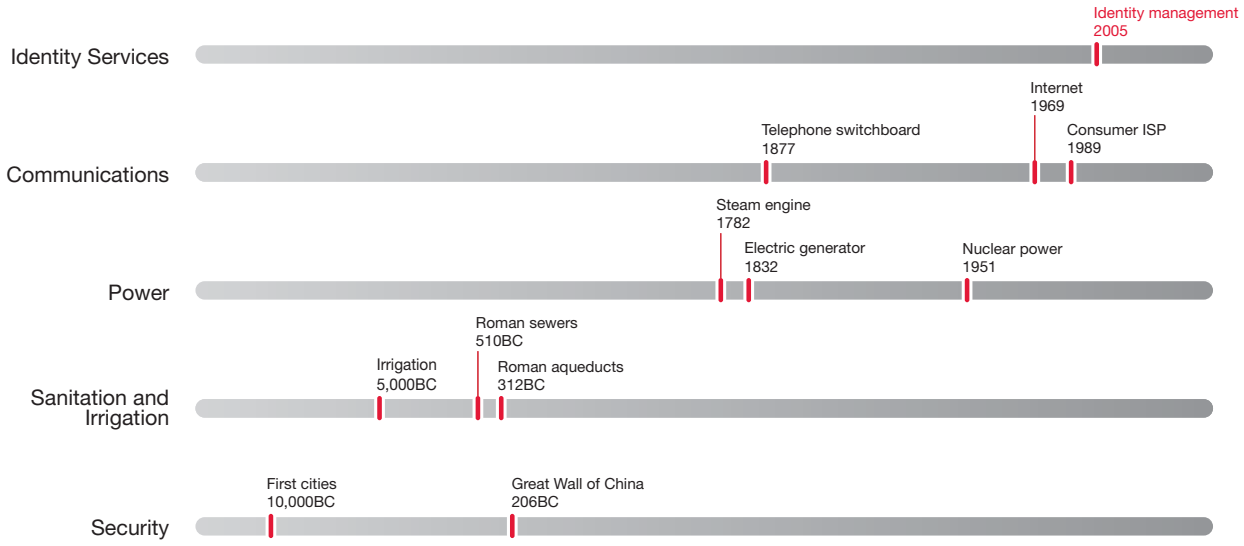

Figure 1: From the earliest days, urban civilizations progressed based on improvements in infrastructure. While the requirement for security remains a constant, other types of infrastructure have become equally important. Identity Services Infrastructure provides the security and convenience required as identity-based applications increase.

As the demand for identity-based services grows, the need to manage them efficiently grows as well. ISI creates a platform for managing these resources.

Identity and infrastructure in the 21st century

ISI enables organizations to create applications that deliver more convenience, security, and privacy with less effort and at a lower cost.

The link between rising standards of living and personal or enterprise productivity has been well established. Productivity is enhanced when people have effortless access to the means of modern production (networks, information and devices) and quick, secure and efficient transactions (personal, cultural, financial or public services). Through ISI, individuals use a single credential that ensures appropriate access. Besides the inherent mobility benefits this provides, it also has a direct impact on the standard of living by enabling people to accomplish more, more quickly and securely.

As the demand for services of all kinds continues to grow, the need to manage them efficiently grows as well. ISI creates a platform for managing these resources. It also provides a way to understand the use of resources in real time. The ability to manage resources adaptively means that service providers can allocate them efficiently and cost-effectively, so more can be done with existing resources.

The move toward ISI today

Today there are many identity-based services, and each requires personal information, carrying with it the problems associated with unnecessary redundancy.

Passports, drivers' licenses, building keys and access cards, car keys, Social Security numbers, IT passwords, credit cards — even grocery store discount cards — all have a fundamental grounding in identity. Each is part of a separate system, and each have different authorization and validation systems supporting it.

The critical transition taking place today is the same one that occurred in other utilities: Economies of scale will drive centralization and consolidation because ISI enables the efficient validation of all types of transactions and supports the centralization of identity, and keeps it trusted and secure.

ISI fundamentals

Identity Services Infrastructure enables people to have access to facilities, services, and transactions anywhere, anytime.

To achieve this, those architecting ISI must consider the following:

- Standards
- Resilient networks
- Credentials
- Privacy and security
- Products and services

Standards

Properly designed ISI doesn't require that all data or network elements be secure. Instead, a distributed system that relies on encrypted information provides very high security over public networks. This lowers the cost and reduces the time to implement ISI.

Resilient networks

Given the critical role played by ISI, networks must be ubiquitous and have high availability—in essence, "always there." The likelihood of consistently delivering high availability is significantly increased because large-scale public networks can be used with no reduction in security.

Credentials

Traditionally, credentials have been viewed as application specific. With ISI, organizations create the platform on which to build additional applications, all of which leverage a single credential.

Privacy and security

The elements that make up the system and the architecture of ISI protect the privacy of users and the security of the transactions. Because of this, rising concerns about security and privacy are two primary drivers of the adoption of ISI.

Authentication

Users are protected against significant loss in the event that their key is lost or stolen by requiring two factor authentication, such as a key and a PIN or biometric.

The authentication requirements for a given activity can be determined based on the type of transaction. Recognizing the high volumes and low risk of individual transactions, a key might be the only thing required when entering a mass transit station. Everyday, but more sensitive, financial transactions, such as withdrawing money from an ATM, would require a PIN, in addition to a card. A large financial transaction might also include the use of a biometric.

Multiple factor authentication including a biometric would be required for high security transactions, such as approval for a police officer to gain access to firearms and ammunition at the beginning of a shift. Providing access to a hazardous materials lab or bank vault could require this higher standard, as well.

Validation

Because the security of any ISI transaction is based on the current status of the participants' credentials, the status (e.g., valid, revoked or suspended) must be checked for every user transaction. As communities grow, this becomes an increasingly high-volume operation. Further complicating the situation is that individuals may have multiple privileges, each managed by a different organization (e.g., immigration services, motor vehicle departments, or employers) which must then be centrally organized for efficient transmission. Naturally, the architecture must address these requirements while maintaining its performance and reliability.

Multiple databases

A fundamental factor to ISI architecture is the fact that there is no central database, and thus no central point of vulnerability.

Logging

Both privacy and security are further enhanced by the requirement that a detailed audit trail is created with every transaction logged.

Application and infrastructure

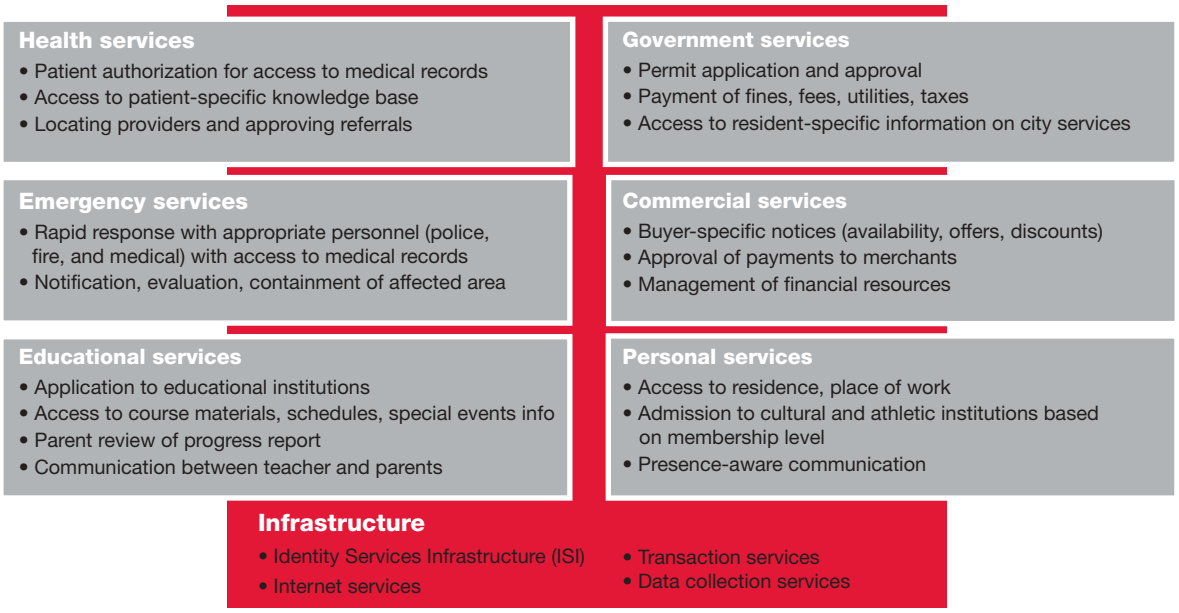

Figure 2: Using Identity Services Infrastructure, organizations can more quickly and economically create applications that are tailored to the needs of individuals and are widely understood to have a very high degree of security.

Products and services

With identity infrastructure in place, applications that deliver more convenience, security, and privacy can be created with less effort and at a lower cost.

Here are a few examples of private sector and public sector applications that would be created on top of ISI:

Business and industry

- Logical access control
- Secure e-mail
- Document signing
- Secure financial transactions

Government

- eGovernment applications
- Electronic passports
- Emergency and First Response
- Physical access to government facilities
- Transportation systems
- Access to public networks
- Government employee access to secure networks and databases
- Driver's licenses
- Hazardous materials transportation permits

In addition, ISI gives organizations the ability to manage access to both physical and information systems through a single system; as a result, users can use the same key to access physical or digital resources.

Case study: Pharmaceutical industry association

SAFE-BioPharma Association is a global identity management coalition founded by AstraZeneca, Bristol-Myers Squibb, GlaxoSmithKline, Johnson & Johnson, Merck, Pfizer, Procter & Gamble, and Sanofi-Aventis.

SAFE (Signatures and Authentication for Everyone) delivers standardized identity credentials that can be used for authentication and electronic signing by the biopharmaceutical and healthcare providers that are members of the SAFE community. These credentials are legally enforceable and comply with industry regulations.

Cost savings from the removal of redundant identity credentials in the biopharmaceutical industry have been conservatively estimated by SAFE to be more than $200 million per year. Current thinking within the industry is that use of digital signatures could help reduce the industry's reliance on paper, estimated at costing the biopharmaceutical industry over $9 billion a year and the health care industry about $500 billion a year.

The SAFE standard is recognized by the Food and Drug Administration (FDA) and the National Cancer Institute (NCI) as meeting federal requirements for Level III authentication and signatures and as being legally enforceable. The European Medicines Agency (EMEA) has evaluated SAFE as meeting all pertinent requirements for EU qualified digital signatures.

The SAFE system is designed to assure the identities of its subscribers and to reduce risks affiliated with creating legally-enforceable digital signatures. According to the association, use of the SAFE credential will allow members to save more than $100 per user per year—a cost reduction of at least 38 percent—in their identity management activities for both internal and external business partners. SAFE is an alternative to multiple and incompatible identity management schemes established by a variety of companies.

The SAFE digital identity comprises policies, procedures, guidelines, technical specifications, and a legal and liability risk management framework. It is being implemented globally for members, and is being extended to members' partners and research organizations in the Americas and Europe.

SAFE-BioPharma Association is encouraging the development of SAFE-enabled software and applications for a wide range of uses within the pharmaceutical and healthcare industries.

CoreStreet's Validation Authority software provides a secure, scalable and cost-effective way for participating organizations to trust every digitally-signed email message and document as well as applications shared with other members. CoreStreet software also makes it possible to instantly revoke an individual's access rights, even if they are not connected to the network at that moment.

Implementing ISI

One of the major driver for deploying an ISI is the need for improved security across multiple identity-based applications. Creating shared infrastructure helps reduce the payback period, by spreading the investment over a large number of potential application providers and consumers.

Distributed architecture

Achieving high performance and high availability in an environment with, possibly, millions of users, all getting data from a small number of sources, has already been studied and solved in the commercial world. The answer is to deploy a distributed architecture. Email and web content delivery are both good example of distributed architectures.

In the case of ISI, validation should also be handled in a distributed manner. There are two key elements to consider when deploying such an infrastructure: (1) There are no constraints limiting the number of certificate status responders (providers); and, (2) no restrictions on the environments in which they can be placed. This is achieved by:

- Quick delivery of credential status by pre-computing all responses
- Securing the integrity of each credential status response so that they can be freely distributed

Figure 3 shows a distributed validation architecture where multiple validation responders have been located close to end user applications without any constraints as to the environment in which they are placed. To accomplish this, the servers must contain no secret information.

Distributed validation architecture for ISI

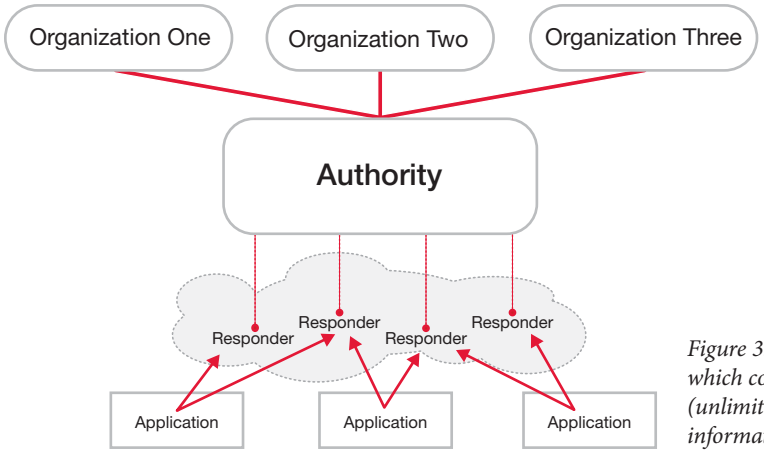

Figure 3: With distributed validation there is one authority which controls the release of validated credential to multiple (unlimited), "secretless" responders that provide this information to applications.

Distributed validation

The central design principle of secure distributed validation is the separation of security sensitive data and trusted operations from the delivery process of providing credential status to the requesting applications.

In this approach, a validation authority contains all the sensitive data and performs all trusted operations. This can be done using a single validation authority, which simplifies the securing of its operations and centralizes its management. Periodically, the validation authority computes individual credential status information and publishes the data. The integrity of the status information can be protected in a number of ways; chief among them is with digital signatures. By digitally signing the data, the following security concerns are eliminated:

- Secure channels for transmission become unnecessary
- The data does not require secure storage

The architecture shown in Figure 4 reflects the fact that within a distributed validation system, responders do not house any security sensitive information and can be placed near end users – in server closets or data centers—thereby ensuring high availability and responsiveness.

There are several advantages to distributed validation

- **Scalability:** High scalability is achieved by decoupling the process for content delivery from important security functions. In doing so, information is secured prior to any requests being made. This eliminate many of the barriers to true scalability – performance, availability, security and cost are thereby eliminated.

- **High availability:** High availability is now achieved because applications have access to a local responder. This is analogous to placing email servers on local area networks to be close to end users for improved availability.

- **High performance:** The distributed validation architecture takes advantage of the lessons learned in the commercial world by decreasing the distance between a relying party application and a responder, eliminating a choke point at the responder, the largest cause of poor performance.

- **Improved survivability:** The single point of failure threat has been significantly reduced. Distributed denial of service (DDoS) attacks are virtually eliminated by the deployment of multiple, geographically dispersed responders.

- **Cost effectiveness:** Since responders do not require secure communication, housing, or operation there is little cost associated with deploying them in a widespread fashion.

- **Flexibility and Adaptability:** Each responder can support more than one validation authority. This allows independent authorities to retain complete control over their domain (i.e., without relinquishing any trusted operations or data to another authority) while sharing a common delivery infrastructure.

- **Improved geographic reach:** Responders can now be located in remote locations without introducing poor performance at the end user due to distance or infrastructure dependent network delays.

- **More secure:** Two elements of security have been significantly improved over non-distributed validation models:

    a. Credential status requests go only to responders, not to the validation authority. Since the validation authority does not allow any inbound communication from the outside world the threat of an outside attack is virtually eliminated.

    b. Scaling the ISI architecture to serve increasingly larger user communities does not require distributing security sensitive data or trusted operations to multiple locations. Therefore, the ability to securely manage this operation is greatly enhanced.

CoreStreet validation infrastructure

CoreStreet validation infrastructure solution offers a distributed credential validation product that can support user populations in the 100s of millions with high availability, high performance, improved security and lower deployment costs. CoreStreet employs a distributed validation architecture and supports pre-computed, digitally signed validation information.

CoreStreet's distributed validation architecture

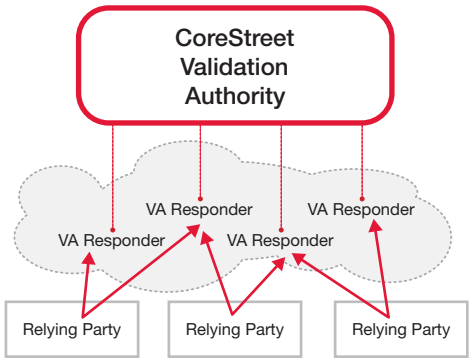

Figure 4: CoreStreet's validation infrastructure ensures scalability without sacrificing performance, availability, security or cost.

Validation information is periodically generated at the CoreStreet Validation Authority (VA) and distributed as digitally signed files to VA Responders. A single VA can easily support a population of 10 million users with daily updates. Larger populations can be supported by simply adding larger and/or additional VA platforms. Each VA Responder is capable of receiving a request for the status of a certificate and returning the appropriate response. Since this operation is a simple table lookup the response is returned in ~2 millisecond. This is a significant improvement over non-distributed validation where each response must be signed before it is delivered to the relying part application.

Benefits

CoreStreet's distributed validation solution provides important benefits over traditional validation systems:

- **Off-line validation:** Because the CoreStreet validation information is unforgeable and unalterable, it can be presented to the relying party application from any source — including by the user himself. This provides great flexibility for applications that are difficult or impossible to connect to a network.
- **Minimum bandwidth solution:** CoreStreet supports low bandwidth environments using MiniCRLs. MiniCRLs offer a factor of 30 size reduction over a traditional Certificate Revocation List (CRL), making them ideal for areas with severe bandwidth limitations
- **Dynamic privilege management:** CoreStreet's distributed validation technology has the ability to dynamically manage multiple privileges associated with a single certificate without having to reissue or modify that certificate in any way. In addition, CoreStreet's technology allows these privileges to be managed by independent, autonomous authorities.

Case study: US Department of Defense

Over the past decade, the US Department of Defense (DoD) has spent considerable time and resources on developing one of the world's largest Public Key Infrastructures (PKI), consisting of over 4 million users with a total of over 13.5 million digital certificates. At the center of the DoD PKI initiative is the Common Access Card (CAC) Program. The program was developed to improve security for all employees worldwide who send email, digitally sign documents and access secure systems.

At the program's outset, small pilot communities found the technology very effective, yet as the user base grew, shortcomings in the original architecture became apparently, namely that it did not scale. Nevertheless, government regulations embraced the security aspects of the technology, requiring that all email be digitally signed in order to validate the authenticity and protect the integrity of the message. Until recently, this process required downloading over 30 megabytes of validation data from a central, secured location which typically took more than an hour to complete. To avoid waiting, many individuals found ways to circumvent the security system, by using alternate email options, such as webmail. With millions of users in the DoD, the cost of lost productivity, as well as new security concerns was significant.

To address the DoD's needs, CoreStreet introduced a new architecture— called Distributed Online Certificate Status Protocol (D-OCSP)—that cuts validation time to 65 milliseconds and requires the download of a file no larger than a few hundred bytes. In addition, the technology provides increased security without necessitating costly, secured responders. In effect, CoreStreet's technology made validation completely transparent to the end user, eliminating many of the concerns brought up by previous technologies.

According to Gil Nolte, Director of the PKI Program Management Office at the US Department of Defense, "People waited so long for CRLs to download that it cost us tremendously in productivity and drove people to circumvent the security built into our systems.

"With the new architecture from CoreStreet, the process is so quick that it is transparent to the user, and we're now able to ensure the security and validity of digitally signed communications."

About CoreStreet

CoreStreet's track record of designing innovative solutions for large scale, high availability identity systems has put it at the forefront of the development of Identity Services Infrastructure. Today, the company's products and technologies are designed into advanced systems built on the principles of ISI and in use today in the Americas and in Europe. The company is based in Cambridge, USA, and has offices in Washington, DC, London, and Milan, and works with representatives in key European markets.

For more information, including detailed product and solution information and technical briefs, see **www.corestreet.com**.

CORESTREET®
An ActivIdentity Company

www.corestreet.com
+1 617 661 3554
info@corestreet.com

Additional whitepapers and datasheets available at:
www.corestreet.com/library

w06-01v2