



The IdenTrust Rule Set: Providing Secure Identities While Protecting Privacy



All You Need is One.
Enabling an eco-friendly digital world.

ABOUT THIS WHITE PAPER

At what point does national security outweigh the privacy rights of an individual or a business? Should an organization incorporated in a European country comply with a U.S. government subpoena for its data?

This debate between privacy versus security is being played out in a highly publicized legal case between a European Union (EU) panel and SWIFT, the Society for Worldwide Interbank Financial Telecommunications. The EU panel charges that SWIFT broke Belgium and EU law by giving the United States government access to SWIFT's transaction records. SWIFT contends that they did not break the law and are in fact caught in the middle of a global debate on privacy versus security.

Through a discussion of the SWIFT/EU situation, this white paper explores how businesses, governments and individuals are increasingly challenged to balance privacy and security issues in an electronic world. This white paper also addresses how the IdenTrust Rules Set enables IdenTrust to protect privacy while still complying with regulatory pressures such as compulsory government subpoenas.

Copyright © IdenTrust, Inc. 2007. All rights reserved.

This document is the intellectual property of IdenTrust, and is protected under the laws of the United States and other countries.

TABLE OF CONTENTS

Introduction	3
Major Study Findings	3
About the EIU Global Online Survey	3
Survey Results	4
Strategic Implications of Identity Authentication	4
The Landscape Grows More Complex	4
Identity Authentication Challenges	4
Conceptual Challenges	4
Implementation Challenges	4
Internet-based Digital Certificates Usage and Shortcomings	4
The Ideal Identity Trust Infrastructure	4
Summary	5
Case Study: France Telecom: The Search for Standards	6
Case Study: LaSalle Bank: Keeping Financial Arteries Clear	6
About IdenTrust	7

In most cultures, privacy is regarded as a basic human right.

If we too easily let down the barriers separating us from either government or corporations, we are risking loss of control that we may come to regret when it's too late to do anything about it.

— Carlton Vogt

THE PRIVACY CHALLENGE

George Orwell's futuristic novel "1984" introduced readers to the concept of a society ruled by "Big Brother." Today, more than twenty years after the fictional novel takes place, technology such as digital certificates, cookies, RFID (Radio Frequency Identification) and biometric scanning enable the sort of surveillance described in "1984."

While most individuals and businesses place a high value on privacy and are aghast at the idea of "Big Brother" watching, terrorism fears sparked by IRA violence in the UK, bombings in the Paris subways, and by the September 11 terrorist attacks have resulted in governments worldwide regulating or offering incentives for businesses to provide them with more and more information about electronic transaction data that can be used in the fight against terrorism.

Privacy as Valued Human Right

Most citizens are in favor of or understand the need for increased security if it means a decrease in terrorism. However, many of these same citizens are unwilling to give up their privacy.

Why is privacy so valued? In most cultures, privacy is regarded as a basic human right. Of course, as individuals we all want to be in control of the type of information that we share with other individuals or even with governments or businesses. In a recent article in InfoWorld titled "Privacy: An Important but Complex Right," Carlton Vogt argues that there are some entities that we as individuals should not share information with.

Writes Vogt, "This group includes those that have great power, are potentially coercive and operate on an impersonal and bureaucratic level: government and corporations. If we too easily let down the barriers separating us from either government or corporations, we are risking a loss of control that we may come to regret when it's too late to do anything about it."

Many share Vogt's view, or at least have questioned the value of privacy and whether the individual right to privacy usurps increases in security. There's no doubt that the privacy debate will continue to heat up.

For example, the Federal Trade Commission (FTC) has recently created the Division of Privacy and Identity Protection, indicating an increased focus on the entire privacy issue. Expect discussions to continue in China and other countries about new privacy legislation. There are no simple answers in the privacy versus security debate and individuals as well as governments and organizations will continue to question the issue.

Data Explosion Fuels Privacy Debate

The amount of data and information that is available to individuals, businesses and governments continues to increase. As more data is collected, information accuracy is critical. Balancing the consequences of decisions made based on bad data against increasing the scope of information inquiries in order to build a larger profile is becoming more common.

Good information management and identity authentication strengthens governance, accountability and transparency. Organizations employing good information practices can minimize information that is false or incorrect.

Since European laws tend to favor the individual right to privacy while the U.S. laws (at least under the current administration) tend to favor national security over the rights of the individual, the U.S. government and EU are at odds.

Only governments can define the boundary between security and data privacy. Private companies, like SWIFT, can play their part by upholding the law, but they cannot make policy and cannot enforce compliance by others.

— SWIFT

EU vs. SWIFT: PRIVACY vs. SECURITY

In recent months, SWIFT has been under scrutiny from the European Union because SWIFT's U.S. branch communicated data to the U.S. government in response to subpoenas from the Office of Foreign Assets Control (OFAC) of the U.S. Treasury. These subpoenas were issued shortly after 9/11 for the purpose of terrorism investigations. According to the Article 29 Working Group, an independent panel set up by the European Commission, answering these subpoenas violated the provisions of the EU Data Protection Directive 95/46/EC.

Since European laws tend to favor the individual right to privacy while the U.S. laws (at least under the current administration) tend to favor national security over the rights of the individual, the U.S. government and the EU are at odds.

SWIFT believes its organization is caught in the crossfire of a global debate on data security that needs to be resolved by governments rather than private industry. In a statement, SWIFT contends, "Only governments can define the boundary between security and data privacy. Private companies, like SWIFT, can play their part by upholding the law, but they cannot make policy and cannot enforce compliance by others. Ultimately they are dependent on governments and elected officials to develop the legal framework in which they operate."

SWIFT does not believe that it has violated data privacy laws, stating that it acted within applicable laws for complying with the mandatory subpoenas from the U.S. Treasury Department.

In addition, SWIFT's argument focuses on its role as a data processor rather than a data controller as defined by Belgium data privacy laws. (SWIFT is incorporated in Belgium and therefore governed by Belgium law.) As a data processor, SWIFT provides a standardized messaging service called SWIFTNet FIN that approximately 8,000 financial institutions worldwide use to perform payment and other transactions across 206 countries.

SWIFT's compliance policy, made available to its customers and published on the SWIFT website (www.swift.com), informs its members that it is required to comply with government subpoenas. Although the EU has determined that Swift had violated European data protection laws, and felt that, "These laws should have prohibited the Belgium-based, financial industry-owned messaging cooperative from complying with this type of request, at least without first obtaining the EU's assent," SWIFT could not wait for that decision before responding to the U.S. government.

These debates will more than likely rage on for several years. As these debates unfold, governments and private industry will need to develop policies and procedures that enable them to protect national security while still protecting data. However, these policies and procedures may have a negative impact in furthering electronic transactions and global interoperability.

In a statement, SWIFT says it is "concerned that Working Party 29's opinion could have far-reaching consequences for SWIFT and other companies providing global information and financial services."

IDENTRUST RULE SET

Like SWIFT, IdenTrust is a members-only network. Its members have agreed to the IdenTrust Rules Set which governs how IdenTrust member banks issue and validate digital identity certificates.

IdenTrust, similar to SWIFT, is a data processor rather than a data controller. IdenTrust's role in electronic transactions is to provide the infrastructure that issues and verifies the authenticity of the digital certificate used by the originator of the transaction as well as to ensure that the receiver is authorized to open the transaction. Like SWIFT, IdenTrust simply passes the message and does not interrogate the message itself. Encryption ensures that the message remains private.

Like SWIFT, IdenTrust simply passes the message and does not interrogate the message itself. Encryption ensures that the message remains private.

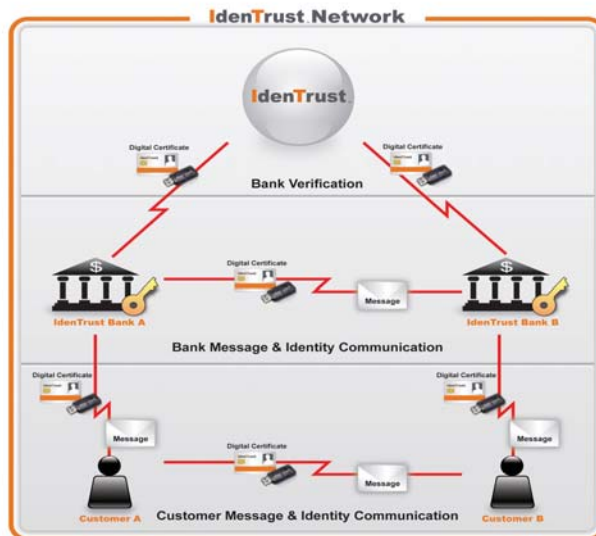
Combining Security and Privacy

Many organizations around the world use digital certificates and access tokens/software that provide high levels of authentication and validation. However, these organizations store the digital certificates and access tokens/software as part of the transaction data. As transactions are opened to perform authentication and verification, privacy is compromised.

IdenTrust does not violate the privacy of the sender or the receiver.

The IdenTrust Rule Set governs the operation of the IdenTrust Trust Network by specifying how a digital identity certificate can be issued and how it is validated. Inherent within the IdenTrust infrastructure and Rule Set is protection against unauthorized access to the transaction information: the IdenTrust infrastructure validates the certificates and only authorized users can interrogate the transaction data.

The transaction data and signed certificate are exchanged between the banks involved in the transaction. The messages related to the transaction data are exchanged between the bank customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust. It remains with the banks involved. Please see the figure below for an illustration of the data flow and the privacy protection inherent within that flow.



IdenTrust is regulated by the Office of the Comptroller (OCC), similar to a financial institution.

All individuals and systems are identified using IdenTrust digital certificates which are specified in the IdenTrust Rule Set. The IdenTrust Trust Network inherently preserves the privacy of transactions to the signer and business application.

IdenTrust does not receive copies of the message traffic between customers or the financial transaction between the banks. The only information IdenTrust receives and sends back to the banks is validation of participant identities.

To perform real-time validation of the signing party, IdenTrust banks require the serial number and name of the issuer of the digital certificate. The IdenTrust Trust Network does not interrogate the transaction content, associated digital signatures or the digital certificate of the signing party. Therefore, the IdenTrust Trust Network has no central tracking function that holds or handles information about the value or content of transactions. In fact, during its initial design, IdenTrust rejected routing transactions through a central point because of privacy concerns.

All validation requests are treated equally using Online Certificate Status Protocol (OCSP) which is real time, or Certificate Revocation List (CRL) technology and protocol. Both are defined in the IdenTrust rule set.

The Governments' Role

IdenTrust financial institution members must perform identification and authentication under government guidelines known in most countries as "Know Your Customer" (KYC) requirements. IdenTrust is regulated by the Office of the Comptroller for Currency (OCC), similar to a financial institution. Therefore, the IdenTrust KYC portions of the Rule Set meet these stringent government requirements and institutions around the world can rely on and trust identities issued under these rules.

As a government-regulated entity, IdenTrust's privacy policy governs the actions of its employees, contractors and vendors. IdenTrust's rule set ensures that the privacy of customer data is never violated since it remains with the banks.

Also, IdenTrust, as a U.S. incorporated organization, must comply with U.S. regulations, including compulsory subpoenas for its data. But since IdenTrust does not store transaction data and only validates the authenticity of digital certificates, a subpoena would not provide the government with access to financial transaction data.

In the IdenTrust Network, no one party is privy to all aspects of the transaction.

Limited Knowledge Increases Privacy

In the IdenTrust Network, no one party is privy to all aspects of the transaction. Limiting knowledge enables IdenTrust to maintain privacy while still ensuring security and authenticity of the identity.

What the Signer Knows

As originator, the signer knows the business application and transactions. The name of the application is contained in the SSL certificate issued by the relying bank and includes one of its certificates in this SSL path. The application sees both names – application and signer.

What the Application Knows

Like the signer, the business application is privy to information about the actual transaction based on IdenTrust rules about what the application must store regarding transactions to invoke the IdenTrust dispute resolution procedures.

While IdenTrust is aware of transactions, there is no technical connection between the banks and IdenTrust.

This IdenTrust Rule Set specifies the information to be kept, but it does not specify the software used to process the information. IdenTrust provides a reference tool kit to application developers so that they can easily become compliant; this tool kit does not contain trap-doors or other routing mechanisms that would expose the transaction to some central process.

What the Banks Know

The issuer bank knows a great deal about the signer. This information is appropriate and necessary for the bank to vouch for the identity of the signer and the credibility of the mechanism used to create the signature. The issuer bank does not know the identity of the application being used by the signer nor does it know the content of the transaction.

Similarly, the relying bank knows the identity of the application, but it does not know the content of the transaction or the identity of the signer.

What IdenTrust Knows

IdenTrust issues credentials to banks and only collects information about whether a bank has checked on the status of another bank or whether one of the bank's customers has checked on the status of their bank. While IdenTrust is aware of transactions, there is no technical connection between the banks and IdenTrust.

CONCLUSION

From its inception, the IdenTrust Trust Network was designed to shield transaction information from undue exposure. IdenTrust combines privacy with an open standard that member financial institutions use to gain global interoperability and legal acceptance in more than 120 countries. By restricting membership to institutions embracing the IdenTrust Rule Set, IdenTrust ensures that the standard is utilized appropriately and in a secure and private manner.

No matter how the SWIFT/EU conflict is resolved, IdenTrust continues to combine privacy with security: no other identity authentication scheme anywhere in the world provides this level of security and identity authentication while still protecting privacy.

ABOUT IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (P.L.O.T.) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, rely on a dizzying maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

Additional information can be found at www.IdenTrust.com.

Corporate Headquarters

IdenTrust Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901

European Office

IdenTrust Inc.
288 Bishopsgate
London, EC2M 4QP
United Kingdom
Telephone: +44 (0)203.008.8330
Fax: +44 (0)203.008.8331

Appendix A: International PKI Standards and Digital Signatures

The digital certificate which uniquely identifies an entity such as an individual, server or corporation provides public key infrastructure (PKI) trust. The IdenTrust Rule Set uses international standards for PKI and the IdenTrust root digital certificate uses secret cryptographic keys to sign certificates for banks and their PKI infrastructure. Banks use these IdenTrust certificates to issue identity credentials and certificates to their customers.

IdenTrust creates a signature that demonstrates that the customer has control of the cryptographic material each time his/her bank issued certificate is used.

The digital signature provides:

- Identification: The certificate identifies the signing individual or server.
- Authentication: The signature could only be created by the cryptographic material in possession of the certificate holder.
- Integrity: The signature proves that the data transmitted has not been changed since the signature was created.

Transactions are executed in the context of an application or business purpose. The digital signature protects transactions, but the application must determine whether or not to trust the digital signature. To do so, the application uses digital signature verification and digital certificate validation:

1. Digital Signature Verification: Mathematical and cryptographic processes local to the business system and the transaction prove authentication and integrity. Using the signer-supplied digital signature and digital certificate, the application can by itself verify that the digital signature is mathematically associated with the digital certificate. The parties of the transaction can identify who originated the transaction and whether the transaction has arrived intact.

2. Digital Certificate Validation: Querying the IdenTrust digital certificate hierarchy to discover the status and validity of the digital identification enables the business process to determine if the credentials (digital certificate) used to create the digital signature have been compromised or stolen.

To determine the current status of the digital certificate, the application needs information from the issuer of the credential. The IdenTrust Trust Network provides the provisioning of this status information.

Appendix B: Example of Transaction Privacy in Procurement Application

The following procurement example illustrates how IdenTrust protects transaction data.

Step 1: Signer logs on to the supplier's web site

Step 2: Signer views and fills in form.

Step 3: Signer activates his/her credentials using a smart card with the stored digital signature.

Step 4: IdenTrust uses these credentials to create a digital signature.

Step 5: IdenTrust attaches the digital certificates to the form to accompany the digital signature.

Step 6: Signed form is sent via the web to the IdenTrust member bank.

Step 7 (or earlier): The application provides an SSL credential that creates an encrypted and confidential session between the signer and the supplier's web server. No one else is able to view this information.

Step 8: The application requests confirmation of the digital signatures' validity.

Step 9: Using the digital signature and the content of the form, the mathematical process of digital signature validation is performed.

Step 10: IdenTrust notifies the application that the digital certificate is still valid.

Step 11: The application creates and signs a request for validation to the supplier's (relying) bank by extracting the issuer name and certificate serial number from the signer's credential.

Step 12: The supplier's (relying) bank contacts the bank that issued the credential via a signed request asking if the credential is still valid.

Step 13: After checking that the supplier's (relying) bank has valid IdenTrust credentials, the issuing bank verifies the serial number of the signer's certificate. The issuer signs a response to the supplier's (relying) bank.

Step 14: After checking that the issuer bank has validated and verified IdenTrust credentials, the supplier's (relying) bank signs and forwards the response to the procurement application. The invoice will be paid.

Step 15: After checking the validity of the supplier's (relying) bank's signed response, the procurement application stores the results of this business operation in its audit log.

The audit log within the procurement application is the only place where the identity of the signer, the identity of the application and the content of the transaction come together.

Appendix C: Knowledge of Transaction Participants

The following table summarizes the information that is known by the various parties in a sample transaction.

	Signer	Procurement Application	Supplier (Relying) Bank	Issuer Bank	IdenTrust
Invoice Form	X	X			
Signer Signature	X	X			
Signer Certificate	X	X			
Signer Serial #	X	X	X	X	
Application Certificate	X	X	X		X
Issuing Bank Name	X	X	X	X	X
Supplier Bank Name	X	X	X	X	X

The table combines some details of the information exchange. For example, there are certificates for SSL between IdenTrust and its banks that keep their communication status confidential. The certificates that IdenTrust and its banks use to sign certificate status responses and requests may be different from those used to sign customer certificates. The information in these infrastructure-level certificates is trusted because it is signed by the IdenTrust root certificate. The transactional information never leaves the signer and the business application.