Who’s on the other end of your transaction?

IdenTrust Partner WebSummit
December 12, 2007
Welcome and Opening Comments

Andrea Klein
Chief Marketing Officer
Agenda

- Introduction
- Update on IdenTrust (15min)
- Case Studies (30min)
  - ISV Partner: XRT
  - Compliant Partner: SafeNet
- IdenTrust Tools (15min)
- Rule Set Update and Partner Implications (45min)
- Q&A / Feedback (10min)
- Closing Comments
Update on IdenTrust

Karen J. Wendel
Chief Executive Officer
Overview: The IdenTrust Value Proposition

- IdenTrust, an Identity Community where …
  - Our banks issue identity credentials usable in more than 100 countries
  - We run an identity validation network that is scalable, self-routing and highly secure
  - We provide tools to embed identity into existing applications

- To do this, IdenTrust provides …
  - Common global standards
  - A global and scalable network
  - High availability, highly resilient hosting services
  - An application framework
  - Portfolio of identity-enabled solutions
Overview: IdenTrust identities play three roles

1. Authentication - Proves identity

2. Encryption - Safeguards content
   - Ensures document integrity
   - Eliminates pharming
     *(man-in-the-middle or DNS poisoning)*

3. Electronic Signing - Replaces ‘wet’ signatures
   - Provides user-level signatures
   - Enables straight-through processing (STP)
     *(paperless workflows)*
Overview: The virtuous circle

More Uses → More Users

More Users → More Applications

More Applications → More Partners

More Partners → More Issuing Banks

More Issuing Banks → More Relying Banks

More Relying Banks → More Uses
Overview: The virtuous circle needs both a cohesive set of products and a market strategy

A Sustainable Platform for All Types of Applications

A Market-Driven Approach for All Types of Business Issues
Overview: A platform that leverages the strengths of all parties

Our Partners are critical because they:

- Provide the key technical elements
  - Hardware
  - Software

- Provide the key business applications
  - Financial Services-centric
  - Supply Chain-centric

- Allow banks and corporates to leverage a common identity platform for multiple use cases

- Identities – even high-assurance identities – are only valuable if they can be used for valuable activities
**Overview: Our market engagement model**

Together, IdenTrust and our Partner Ecosystem can:

- Create demand for not only identities, but also applications
- Provide new ways to address long-standing business pain points
- Deliver compelling revenues and/or cost reductions to all participants in the “triangle”

*in conjunction with our Partners*
Customer Case Story

Jean Beaufort, Managing Director
Jose Teixeira, Corporate Senior Product Manager
XRT and IdenTrust - Accountability and Trust for Payments Workflow
XRT  The Reference for Financial Value Chain Solutions

- 20 years of innovative solutions for Financial Value Chain Management
- Used by 6000 companies including 500 large corporations in 55 countries
- Complete Financial Value Chain Management:
  - an optimization of working capital and cash
  - foreign exchange and interest rate risk
  - receivables management and collection
  - centralization and automation of payments and bank communication
- IdenTrust and SwiftNet enabled
XRT The Reference for Financial Value Chain Solutions

XRT provides a global & real time visibility on all financial flows within the organization: Financial Value Chain Management

- Optimized Working Capital Management
- Improved client & supplier relationships
- Reduced transaction processing costs
- Improved risk management
Our Solutions

- **XRT Universe**
  A flexible and modular solution that covers the full Financial Value Chain from Collection to Payments

- **XRT Business Exchange**
  A secured electronic banking and financial information exchange platform for large corporations and banks
XRT Business Exchange is a secured electronic banking and financial information exchange platform for banks and corporations that wish to build payment and collection factories.

**Product application overview**

**Various functionalities**

- **Bank Exchange Services.** The ability to communicate securely as server or client with any other remote (bank) server. Many local and international protocols and formats supported. Follow-up of communication & workflow, with alerts, automatic triggering of communication at events, scheduling.

- **Connect for ERP.** The ability to securely communicate with ERPs for payments and statements. SAP certified.

- **Web Payment Services** The ability to import payments from ERP systems, to enrich information if incomplete; input of urgent payments; payment centralization (factory) functions, redistribution over different banks and entities, or netting of payments; flexible approval workflow for payments. Local and international payment formats are supported.

- **Web Signature Services.** Electronic sealing of messages. Can also be used for a strong internal approval workflow. All currently used electronic signatures are supported, including hardware.

- **Web Bank Services.** The ability to have a consolidated reporting on information coming from banks, such as bank statements.

- **Web Documentary Credit Import / Export.** A solution to keep track of documentary credit and the events in the lifecycle of documentary credit. Both import and export situations are covered.
Build your Payment Factory

Subsidiaries

ERP

Shared Service Center

Business Exchange Services

Connect for ERP
Payment Services
Signature Services
Bank Services
Credoc Export
Credoc Import

Banks

Local Financial Network

Internet

Swiftnet
A Unique Value Proposition to Build a Secure Payments Workflow

- **100% web based**
- **All types of payments, with adapted workflows and authorizations**
  - Bulk Payments:
    - Accounts Payable
    - HR Payments
  - Urgent Payments
    - Treasury
    - Last Minute
- **A complete payment factory offering full STP**
  - Workflow automation, depending on payment type
  - Enriching of ERP (imported) payments
  - Routing, bank / payment type quota management, netting of payments
  - Payments and Requests for Payments (payments on behalf of a subsidiary)
  - Manual input of urgent payments & template management
  - Validation and authorization cycle
  - Bank format generation
  - Audit, ledgers & statistics reporting

- **Notification Services**
- **Real-time payment dashboards**
- **Reports**
XBE: The Signature Process with IdenTrust

- 100% web based
- Trust is a key issue for the growth of electronic exchanges
  - Build a strong legal approval chain through electronic sealing of messages
  - Signatures can be internal or external - transmitted to the banks or other partners
  - A unique workflow based on sophisticated signature rules (based on amounts, transaction types, banks, limits, ...)
  - Notifications and alerts, priorities in sending emails to the signatories
  - Ledger, audit and signature proof management for legal purpose

- XRT and IdenTrust will provide a unique Trusted Workflow for your payments
IdenTrust Partnership

**XRT’s Interest**
- We try to get XBE IdenTrust certified, in order to extend the XRT offer. IdenTrust certificates are accepted by an increasing number of banks. First focus: Payment Signature and Validation over SwiftNet.
- IdenTrust may have a role to play in SEPA – they are the only ones to be able to provide interoperable certificates. So a smartcard issued by one bank can be used to pay for another bank as well, just like Etebac 5.

**IdenTrust’s Interest**
- to have applications that accept IdenTrust certificates
- XRT customer base (Corporates and Banks)
Reconnecting and early re-engagement in January 2007

- NDA & ISV agreement signed in 2007
- Decision to schedule the Certification Process
  - Target: 2008 SEPA Release
  - First Focus: Signature over SwiftNet
  - Define the team
  - Work closely with IdenTrust team (technical, Marketing and Sales)
- Press release to announce the partnership
- Press releases with IdenTrust announce:
  - IdenTrust Partnership Press Release
  - SWIFTNet Certification
  - SEPA Ready
- Cross Marketing and joint Events
  - SIBOS
  - BNP Cash Management University
IdenTrust – XRT Marketing & Communication (2)

- **AFTE (French Treasury association event)**
  - Press Release / Demonstration  SEPA Ready and IdenTrust Enabled for Signature & Identity management

- **Payment Centralisation & Security  XRT Event**
  - 40 Corporates attended

- **Respond to first RFPs with confirmed IdenTrust compliance**
  - First presentation to prospects done
  - First joint meeting with customers organized /scheduled

- **Introduction / discussion with Banks**

  We will Launch the certified release with the official Launch of SEPA in Europe
Market Opportunities

- **SEPA**
  - SEPA is a driver for centralisation
  - Payment Institutions evolutions
  - Security (identity and Signature) the key point

- **Financial Value Chain**
  - Opportunités in full financial value chain scope, notable e-invoices and reconciliation
  - As the financial value chain becomes paperless, electronic identity management & Signature will become an issue (again)

- **Centralisation is still going on, and goes mid market**
  - The Market and the opportunities will grow

- **The EU 8th directive ("European SOX") will become local law**
Customer Case Story

Dave Madden
Director of Business Development
IdenTrust Partner Webinar: SafeNet Overview
Agenda: IdenTrust & SafeNet

- SafeNet company & solutions overview
- Identity and access management market trends
- Why tokens vs software key protection?
- Customer Deployment examples with IdenTrust:
  - Financial requirements for Digital IDs
  - Safe Certificate Use for the Pharmaceutical Industry
  - Federal ECA mandate
- Other Examples of deployments
SafeNet, Inc. Overview

- Encryption experts with 23 year history of protecting:
  - Data at Rest & in Motion
  - Intellectual Property Rights
  - Digital Assets and Identities

- Global Company with Local Service
  - Headquartered in Maryland, USA
  - 30+ offices located in more than 20 counties
  - Partners in an additional 100+ countries

- Encryption technology heritage
  - 43 patents issued, 31 patents pending
  - Majority of the leading security vendors embed SafeNet’s technology in their offerings

- Fastest Growing Networking Company – 2005
- IdenTrust Partner since 1999

Source: Networking Magazine
Acquisition History

- SecureLink
- eracom Technologies
- DataKey
- CYLINK
- SafeNet
- RAINBOW Technologies
- DMDsecure
- mediaSentry
- raqia networks, inc.
# SafeNet Product Portfolio

## Identities
- **Authentication, Remote Access, and Compliance Enforcement Products**
  - **ID Tokens and Middleware**
    - Borderless Security 330 Smartcard
    - Borderless Security iKey 1000 and 2032 (USB token)
    - Borderless Security Single Sign On
    - Borderless Security Carc
    - Management System
  - **ID Management**
    - Luna HSM
    - Protect Host
    - Protect Server
    - API Toolkits
    - Command Interfaces

## Communications
- **Encryption Products**
  - **Data in Motion – Bulk Encryption**
    - Ethernet Encryptor
    - SONET / SDH Encryptor
    - ATM/Frame/Link Encryptors
  - **Data in Motion – Remote Access**
    - High Assurance IPSec Gateways
    - High Assurance VPN Clients
    - Borderless Security SSL iGate (SSL VPN)
  - **Policy Management**
    - Security Management Center
  - **Data at Rest**
    - ProtectDrive
    - ProtectFile
    - Protect Pack

## Intellectual Property
- **Rights Management Products**
  - **Anti-Piracy and License Management**
    - Sentinel RMS
    - Sentinel Hardware Keys
    - Unified Software Protection
  - **Content Protection**
    - MechaSentry services
  - **Digital Rights Management**
    - DRM Mobile
    - DRM Fusion

## Embedded Security Products for OEMs
- **VPN/IP/FW Software**
  - QuickSec for Unified, Unified IPSec, Unified Anti-Virus, Telecom, IKEv2
- **Semiconductor IP**
  - SafeXcel IP Security Engines
Security Market Drivers

- **Privacy** -
  - External Driver - breaches in current security raise publicity and create external push to improve data security and privacy protection.
  - Internal Driver - push from within to enable programs & reduce cost of breaches

- **Mandates**
  - Global Transaction Services Banking
  - IdenTrust PLOT Model
  - SAFE Pharmaceutical Consortium and legal framework
  - Payment Card Industry Data Security Standard (PCI-DSS) to process card payments prevent credit card fraud,
  - ECA Program for DoD partners, suppliers and contractors
  - HSPD-12 Mandate for US Federal
  - Sarbanes-Oxley - (SOX) - US federal law passed in 2002 in response to corporate scandals around accounting and reporting. Some of the numerous requirements under SOX include:
    - Gramm-Leach Bliley - allowed commercial and investment banks to consolidate. Goal is to protect the clients. Must have safeguards in place:
Why store IdenTrust certs on tokens?

- **Increased security:**
  - A PIN is required to use the private key on the hardware
  - Private keys are always protected in hardware and cannot be stolen, copied or shared with coworkers (inadvertently or deliberately)

- **Regulatory compliance:**
  - Many standards such as HSPD-12 requires protection of user’s ID with 2 factors:
    - physical security of the private key &
    - something you know, a PIN

- **Employee accountability**
  - Non-repudiation: if only the employee has control of their key in hardware, then they alone could perform the signing of a transaction or email or document

- **ID Mobility**
  - All your authentication on one mobile device that you can move from one computer to another
Credit Card-like or USB Dongle form factor
- 64Kb EEPROM User memory
- Same chips used on either iKey 4000 or SC 400 products
- Proprietary multi-file card OS
- HW and SW protection against differential power and timing attacks
- Physical & Logical Access Control
- Supports AES in addition to the algorithms supported in SC 330
- Strong Security
  - FIPS 140-2 Level 2 compliant (validation in process) (Level 3 for iKey 4000)
  - CC EAL 4+ for iKey 4000
- Simplified variants
  - Unblocking capability is a standard feature now
  - Match on Card biometric authentication support*
  - Identrus support is available natively on SC 400 / iKey 4000
  * Biometric support requires additional premium in software due to licensed technology

PKCS#11 & CAPI API for integration with applications
Customer Initiatives with IdenTrust

The following initiatives often coincide with smart ID deployments:

- Compliance With Regulations: storing keys securely & 2F Auth
- Homeland Security: PIV compliance & ECA Program
- Upgrading a new physical access system: Physical & logical access on one offering
- The need to solve a password management problem: SSO
- Remote access security (VPN)
- New business initiative to let employees, partners, or suppliers get access to their information: Web Portals
- eDocuments: signing email, transactions or documents electronically
- Laptop Security Incident – sensitive information lost, or compromised: Disc Encryption & preboot authentication
Global Transaction Services (GTS): GTS offers a trusted intermediary for certificate services on behalf of its partners and customers.
SAFE enables the move from paper to electronic processing of new drug submissions.

IT Infrastructure

Signed Documents

OCSP

IdenTrust PKI: Safe Policy

Safe: ID Mgt & App Sec

Pharma, FDA, Lab or Doctor

Document Protection
Access control/SSO
Secure Email
Payment Processing
Encrypted hard drive
SafeNet & IdenTrust Overview for ECA

ECA enables: Identity authentication, Digital signing, and Encryption & Key Escrow for Encryption keys

Federal Industry Partners & Consultants
t-Certificates

Federal Agency Access with ECA

ECA Programs:
Wide Area Workflow, Defense Travel System, and the Secure Messaging and Electronic Document Access

Documents & Email

OCSP

IdenTrust PKI: DoD Policy
Examples of New ID Security Initiatives

- Credit Card PIN management online
- Swift Banking Infrastructure
- Paper to Digital processing and clearance
Customers can change and update their Credit Card PIN online in a secure manner.

1) User enters the Card Verification Value (CVV)
2) The CVV is encrypted
3) The CVV is forwarded to the card issuer via the bank web portal
4) The PIN associated with the account, is sent through the bank web portal for VPS decoding
5) The VPS then decrypts the PIN and displays the pin to the user over the SSL sever
SafeNet – Securing Banking Transactions

Small Banks

Access Control via 2 or 3 factor

SafeNet HSM
Key Management
SSL Acceleration
FIPS certified

Financial Transaction Infrastructure

Large Banks

SafeNet HSM

Applications

Payments & Cash Mgt
Treasury & Derivatives
Trade services
Pre-Settlement/trade
Clearing services
Custody services

Certificate Authority

Directory

SafeNet HSM

SafeNet – Securing Banking Transactions

SafeNet – Securing Banking Transactions
Check Clearing Process
Embedded Example

- **User Auth**
  - Luna PCI
  - Root Key Storage, Signing, Encryption

- **Clearing House Interface (Presenting Bank)**
  - Check MIRC data & images are captured at the Presenting Bank

- **Clearing House**
  - Inward Check MICR & images
  - Signed & Encrypted
  - Outward Electronic Check
  - MICR & image

- **Sign & Enc data**
  - OCSP & Enc data
  - Auth & license control

- **Luna SA**
  - Luna PCI
  - Root Key Storage, Signing, Encryption

- **Auth & license control**
  - Database encryption

- **Clearing House Interface (Paying Bank)**
  - Outward return Check MICR
  - Signed & Encrypted
  - Outward Electronic Check
  - MICR & image

**Electronic Check Archive**
Why Customers Deploy IdenTrust & SafeNet

- IdenTrust compliant solution in accordance with PLOT
- Broad interoperability with applications via standard APIs
  - Standards-based
  - Certificates + Tokens for 2 Factor Authentication
  - Identity authentication, Digital signing, and Encryption
- Security certifications
  - FIPS level 2 & 3
  - CC in preparation
- Strong IdenTrust & SafeNet partnership
Contact Information – for any question

Dave Madden - IdenTrust Partner Manager

- [dmadden@safenet-inc.com](mailto:dmadden@safenet-inc.com) & 613-221-5016
IdenTrust Tools

Rama Thamman
Director, Delivery
IdenTrust Tools

- **Client side integration tools**
  - Universal Signer
  - Trust Sign

- **Server side integration tools**
  - DSMS toolkit
  - Super DSMS Server

- **Testing Tools**
  - Smart Card Test Suite
  - Relying Customer Tests
Universal Signer is a Java based Applet that can be easily integrated with web applications for creating digital signature. As the name suggest, this tool can not only be configured to create signature to comply with IdenTrust specifications but also to other standards.
Universal Signer, Cont’d…

- Eliminates the need for installing vendor plug-in software for accessing certificate storage devices
- Highly configurable – Key usage, Object Identifier settings, etc.
- Supports text based (PKCS7) or XML-DSig based signature creation
- Supports certificate validation capability before signature creation
- Supports on-demand signature validations as a stand alone utility
- Supports basic encoding formats
- Requires Java Runtime Environment version 6.1 or newer on the client machine
The TrustSign solution enables corporations, financial institutions, and government agencies to prepare, sign, and deliver business-authenticated, trusted documents over the Internet.

Process overview:
Trust Sign, Cont’d…

- Works in conjunction with Adobe Reader or Microsoft forms
- Support for static and dynamic forms
- Globally Interoperable Electronic Form
- Real-Time Signature validation
- Non-Repudiation and legal binding
- Easy to use - Point and Click Signing
- Document control and security – prove that documents have not been altered using built-in tamper controls
- Reduced Operating Costs
TrustSign, Cont’d…

**Certification** - indicates that the document is truly from the bank

This is a digital signature from the bank – either from a named individual or uses a “corporate” entity certificate

**Digital Signature** - The signature block contains all the information needed to verify signature. It is created by the signer utilizing their IdenTrust digital certificate and associated PIN
DSMS Toolkit

- DSMS toolkit is a set of libraries necessary to configure a Web Application to accept digitally signed data, to verify a digital signature or to validate a certificate, all in compliance with IdenTrust specification.

- Built using IAIK Java Cryptography Extensions (IAIK-JCE)

- Implemented in 100% Java

- Developed to run in a Java 1.4 and higher JVM
DSMS Toolkit, Cont’d…

- Accelerates certificate enablement of Web applications and reduces integration costs
- Easy to integrate with any J2EE Web application just by configuring a few parameters
- Provides interfaces to access a hardware security module
- Supports signing and verification of data under PKCS7 and XML-DSig specifications
- Supports creation of parallel signatures (Co-signer)
- Robust logging and debugging capabilities
- Can be implemented in transaction processing or batch mode
- Can be deployed on a server or a desktop
Super DSMS Server is an IdenTrust hosted and managed service to perform digital signature verification and certificate validation.
Off the shelf IdenTrust compliant enablement of web applications to process IdenTrust certificates and those of other PKI systems

- Supports IdenTrust style signature validation as well as other types. For example, RFC 3280
- Archive and retrieval of signed transactions and validation status
- Digital notarization support
- Supports signed and unsigned Online Certificate Status Protocol (OCSP) validations
- Toolkit is available for interfacing with the server
- HSM hosting support
Testing Tools

- **Smart Card Test Suite**
  - IdenTrust maintains a website that can be used by KSM vendors to test for compliance
  - Both ISPI and ISIL compliance tests are supported

- **Relying Customer Test**
  - Web based tool for testing KSM devices in a relying customer setup

- **General Purpose Utilities**
  - A set of general purpose tools to assist compliance certification. For example, parsing a signature object, etc.
IdenTrust Tools Collateral

IdenTrust Tools

- Certificate Enablement Toolkit
- Universal Signer
- DSMS Server

Datasheets for the IdenTrust Tools can be found at:
www.identrust.com/info_center/collateral
Rule Set Update and Partner Implications

Vish Patel
VP, Product and Rule Set
Due to IdenTrust confidential information, we cannot publicly publish this content. If you would like more information on the Rule Set update and its implications to our partners, please contact:

Knud Balsev, Director of Global Alliances
knud.balslev@identrust.com
(415)486-2907
Q&A
Closing Comments

Thank you for participating in the IdenTrust Partner WebSummit!