



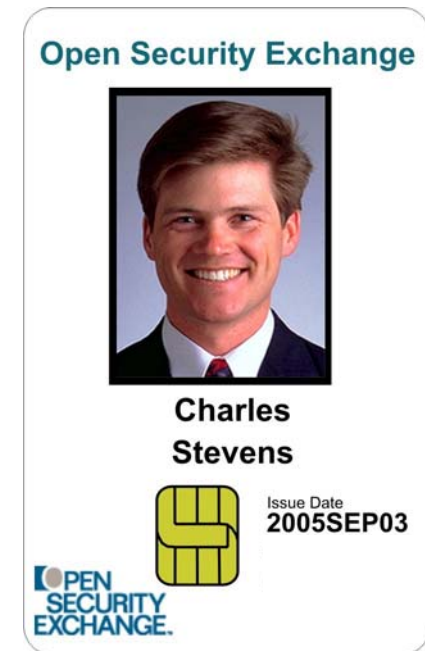
# **Combined Credentials for Physical and IT Security**

**August 12, 2005**

# Combined Credentials

Combined Credentials for physical and IT security lay the foundation for efficient and intelligent security.

- ❏ Who Needs a Combined Credential?
- ❏ What is a Combined Credential?
- ❏ Why is a Smart Card Recommended?
- ❏ Combined Credential Card Readers
- ❏ Levels of Security
- ❏ Provisioning and De-provisioning
- ❏ Benefits of the Combined Credential
- ❏ Success Factors
- ❏ Where to Get More Information



# Who Needs a Combined Credential?

- ❏ Need to Protect Financial Data?  
Banks, Insurance Companies, Investment Companies
- ❏ Need to Protect Information Assets?  
Multinational Conglomerates, Software Companies, Lawyers
- ❏ Need to Protect Physical Assets?  
Pharmaceutical Companies, Manufacturing Companies
- ❏ Need to Protect Private Data?  
Banks, Data Clearing Houses, Doctors
- ❏ Need to be Compliant to Regulations?  
Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, HSPD-12



We all have physical and IT security concerns, but it is employees who bridge the physical-IT gap

# What is a Combined Credential?

Combined Credentials provide the glue that holds enterprise security together at the employee level

- ❏ Identify the Card Holder

Photo, biometric, certificates, PINs, passwords, employee number, affiliations.

- ❏ Security Assurance

Standardized format and interoperability assure common credential practice e.g. X.509 certificates.

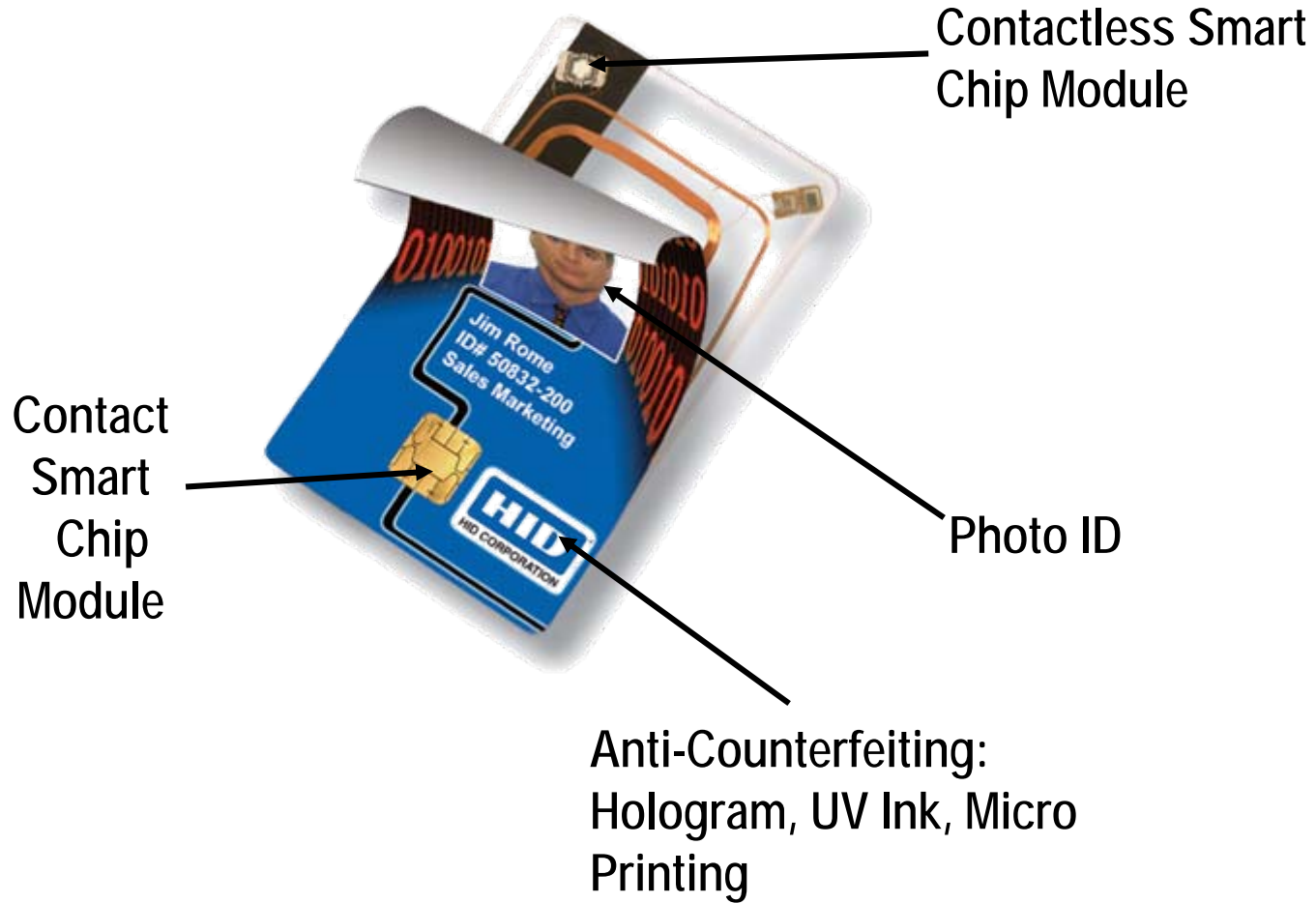
- ❏ Systems Access

A combined credential provides a single device for accessing IT and physical systems.

- ❏ Both Electronic and Visual Validation

Certificates, PINs, passwords, and biometrics securely stored on a Smart Card are used to validate both the card and the holder. Photo identification with holograms, micro-printing and covert security provide visual validation.

# What is a Combined Credential?



# Why is a Smart Card Recommended?

Smart Cards provide the kind of portable intelligence required to implement Combined Credentials.

## ✧ Identity Authentication

A Smart Card is a personalized computer that uniquely identifies you to multiple computerized security systems in a secure manner that maximizes privacy protection.

## ✧ Encryption Technology

Because a Smart Card has encryption capability, it can facilitate secure communications using PINs, passwords, certificates, and biometrics.

## ✧ IT Access

Smart Cards securely and efficiently manage the biometrics, passwords and certificates you may need for accessing IT systems on a single card.

## ✧ Physical Access

A Smart Card provides easy access to multiple facilities as well as updating privileges for remote or disconnected areas.

# Combined Credential Card Readers?

## ❏ Contact Interface

Contact readers for Smart Cards are usually used for IT access.

## ❏ Contactless Interface

Readers for contactless Smart Cards are usually used for physical access.

## ❏ Card/Reader Standards

ISO 7816 is a mature standard that covers all of the necessary physical and communication parameters needed to interface with and perform operations on contact chip credentials.

ISO 14443 and 15693 are standards that detail communications using contactless credentials. There are several implementations of the contactless standards which decrease interoperability. A movement towards standardized ISO 7816 command sets over contactless interfaces is underway.

**Networked card readers and systems lay the foundation for increased efficiency and intelligent security.**

# Levels of Security

## α Security Factors

Commonly accepted Security Factors are: What you know; What you have; and Who you are. In the Smart Card you have one or more stored certificates, PINs, passwords, or biometrics. Cryptographic capability on the Smart Card keeps them secure.

## α Security Levels

Some applications facilitated by a Smart Card require a very high level of security. Using something you know like a PIN along with a biometric that uniquely identifies you comprises 3 Security Factors.

## α Physical and IT Access Security

At least 2 Security Factors are recommended to protect sensitive assets because it is much harder to compromise. Some less sensitive applications may only use 1 Security Factor like a Smart Card or a biometric.

## α Interoperability for Security

Many organizations are finding the need to authorize people who are not their employees. Emerging standards for Smart Card Interoperability will enhance security when collaboration is necessary.

# Provisioning and De-provisioning

Enterprise-wide de-provisioning eliminates important security gaps that exist between systems

## ❏ Security Systems Coordination

It is recommended that all of the databases in an enterprise be coordinated to facilitate the highest level of security for all applications across the enterprise.

## ❏ Certificates and Card Issuance

Multiple certificates are for authentication, digital signature and encrypting documents. De-provisioning involves revoking one or more certificates.

## ❏ Standard Employee Data Format

Two emerging standards for smart credentials are ISO 24727 and FIPS 201.

## ❏ Remote Provisioning Support

Remote privileges can be supported on a Smart Card by providing privilege information to a stand alone device or system.

# Benefits of the Combined Credential

## ⌘ Increased Efficiency

Improved efficiency in IT access due to improved password management, less time to investigate breaches in security because of single enterprise-wide provisioning, and consolidation of physical and IT security assets.

## ⌘ Intelligent Security

When computer access, building access, and surveillance are all accessible by a single IT application, the possibility exists to set business rules that detect security events which would otherwise go unnoticed.

## ⌘ Interoperability and Cross-Credentialing

Standardized combined credentials build a foundation of trust between systems and organizations as well as operational efficiency.

## ⌘ Enterprise-wide Provisioning

A Combined Credential facilitates enterprise-wide provisioning that eliminates gaps between security systems thereby improving security efficiency.

# Benefits of the Combined Credential

- ❏ Access Control Savings

Save the cost of having guards, managing keys, or managing multiple credentials for multiple sites with different access systems.

- ❏ Higher Security

Many levels of authentication are possible with certificates and encryption.

- ❏ Compliance Audit Trail

Gramm-Leach-Bliley Act, HIPAA, Sarbanes-Oxley Act.

- ❏ Password Management

Smart Cards facilitate user password management preventing weak passwords and passwords posted in plain view.

- ❏ Password Reset Costs Savings

Estimated savings of \$150+ per year per user. 90% reduction in password reset calls at the DoD after biometric logon deployment.

**You can save money and save your enterprise from an embarrassing security event?**

# Success Factors

The experience of others has shown that the following factors can influence success:

- ❏ **Top Management Sponsorship**

An executive champion can provide the consistent support needed to maintain momentum for a project spanning multiple business cycles. .

- ❏ **Involvement and Collaboration Across Security Organizations**

A Combined Credential requires converging security visions, policies, processes, and technologies across multiple organizations such as: IT security, physical security, and audit. Look for ways to share ideas, obtain resources, and manage risk across formal organizational boundaries.

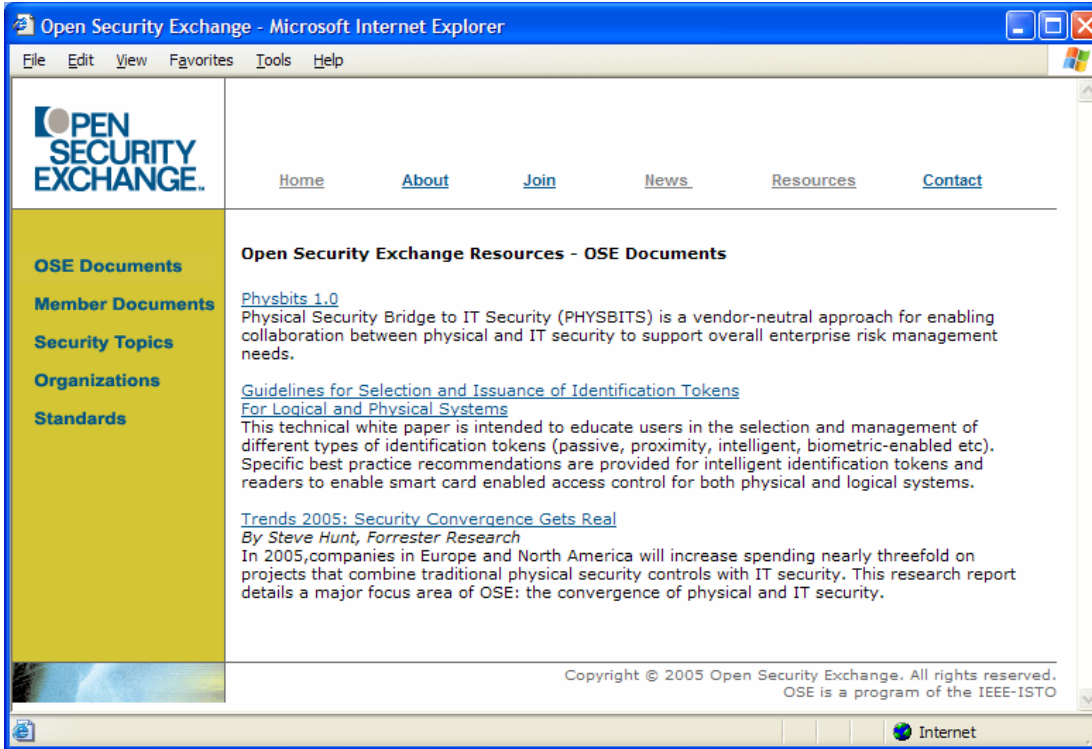
- ❏ **Robust Enterprise Directory Implementation**

A single fully populated accurate enterprise store of credential information will reduce the scope and complexity of a Combined Credential project. Draw from all personnel systems, e.g. employees, contractors, etc.

- ❏ **Standardized Infrastructure**

Standardization of workstation platforms, electronic software distribution, and physical access control systems will streamline a Combined Credential deployment.

# Where to Find More Information



- ✦ OSE Documents
- ✦ Member Documents
- ✦ Security Organizations
- ✦ Links to Security Information
- ✦ [www.opensecurityexchange.org](http://www.opensecurityexchange.org)
- ✦ [info@opensecurityexchange.org](mailto:info@opensecurityexchange.org)

## Contributors:

Sal D'Agostino – CoreStreet

Andy Bulkley – GE

Peter Borskin – Software House

Piers McMahon – Computer Associates

Nathan Cummins – HID

Gary Klinefelter – Fargo

Bill Nuffer – Deister

# OSE Membership

## Board Members



Computer Associates\*



## General Members



## Convergence Council Members





# Questions

