Physical Access Control Solutions

HID Global

The market leader for trusted identity solutions by providing seamless access leveraging a connected architecture complemented by cloud services

Powering the trusted identities of the world's people, places & things

Keys Today

Each use case is a discrete ecosystem of readers/locks/ applications and access keys.

Key formats have been specific to the individual ecosystems.

RFID cards

Metal Keys

Passwords

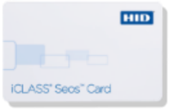
Visual Documents

Infrastructure for Tomorrow’s Keys

Keys will no longer be bespoke pieces of hardware, such as brass keys or dedicated plastic cards.

Instead there will be digital keys that can reside on a variety of smart devices – mobile phones, micro-processor cards, wearables.

Microprocessor cards

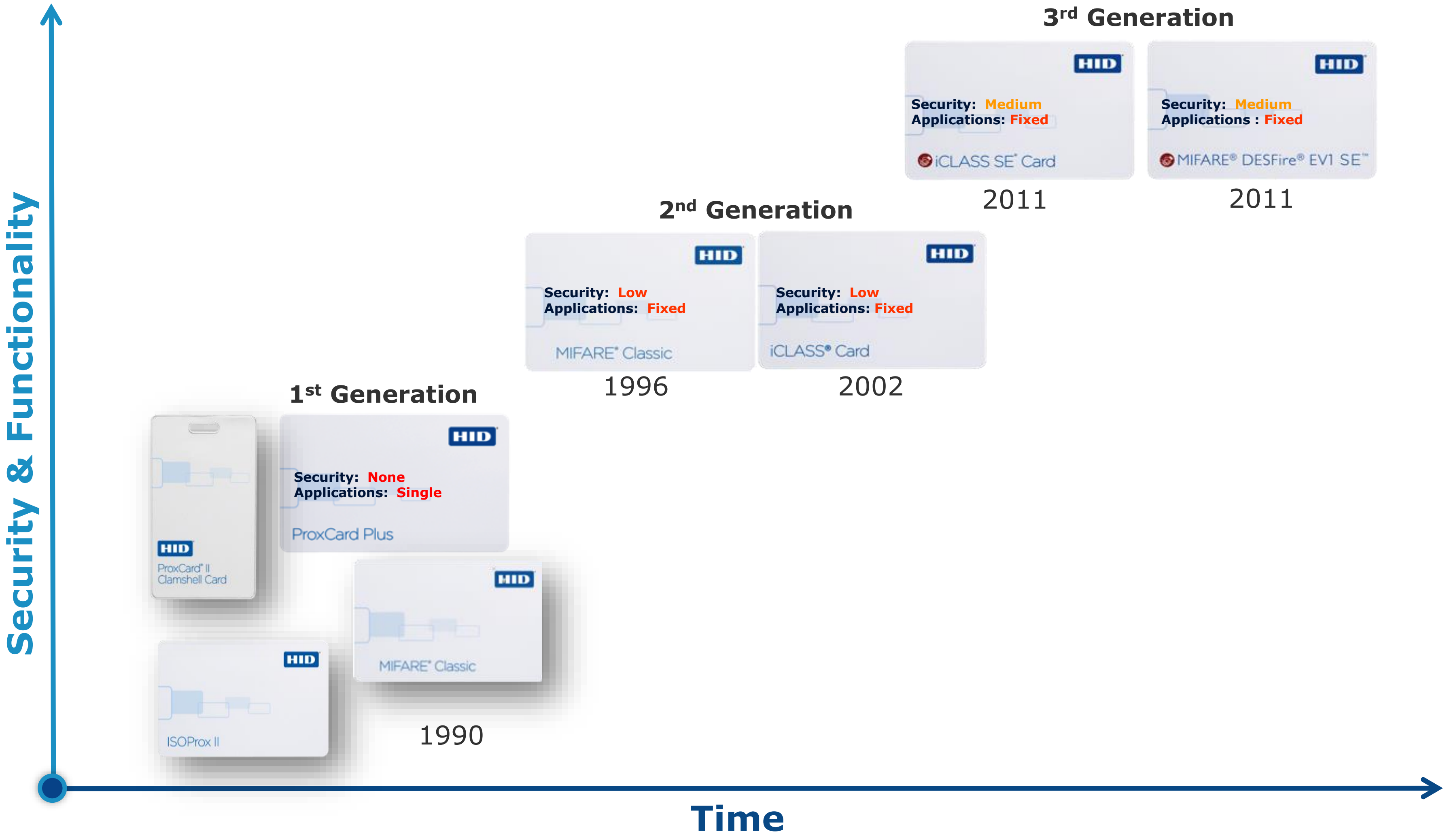


Smartphones

Wearables

Biometrics

Evolution of Credential Technology



3rd Generation

Security: Medium
Applications: Fixed
2011

Security: Medium
Applications : Fixed
2011

2nd Generation

Security: Low
Applications: Fixed
1996

Security: Low
Applications: Fixed
2002

1st Generation

Security: None
Applications: Single

1990

Is the Card Really Secure Enough for Secure Access Control?

125 kHz

Not anymore

13.56 MHz

It depends on:

- Technology used
- How it is used
- How the data are provisioned

The Problem with the Status Quo

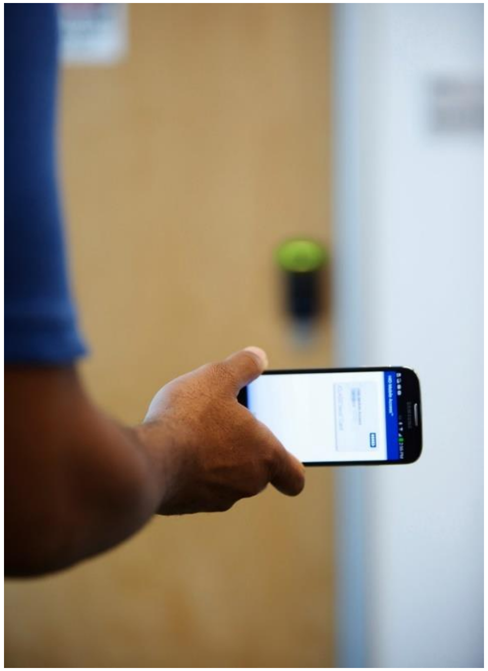
Vulnerabilities

- Using Standard or Default Keys
- Failing to encrypt or digitally sign the data payload
- Using open, non-tracked card formats
- Configuring readers to support secure credentials alongside legacy
- Allowing unencrypted communication to the panel

The Problem with the Status Quo

Summary

- Security vulnerabilities in technology and/or implementation
- Limited support for multi-application
- No path to mobile access

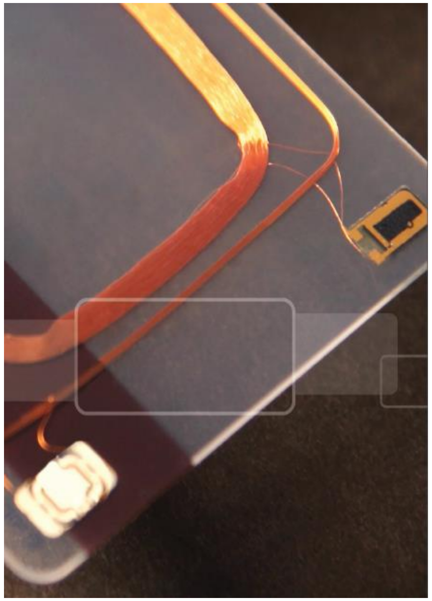


A Holistic, Secure Credential Program

More confidence

Secure technology is foundational:

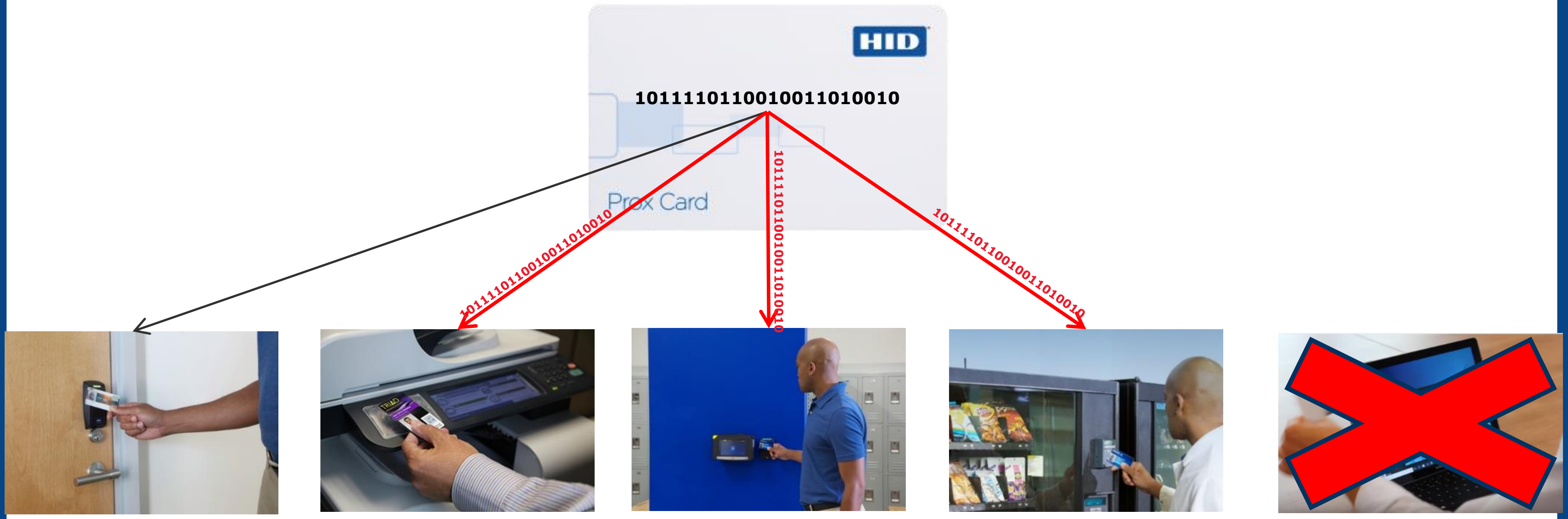
- Standards-based cryptography
- Credential technology independent of underlying hardware chip
- Enhanced privacy protection with no unauthenticated access to data



Secure **Technology** is Foundational

The Problem with the Status Quo

Multi-application



1011110110010011010010

Physical Access

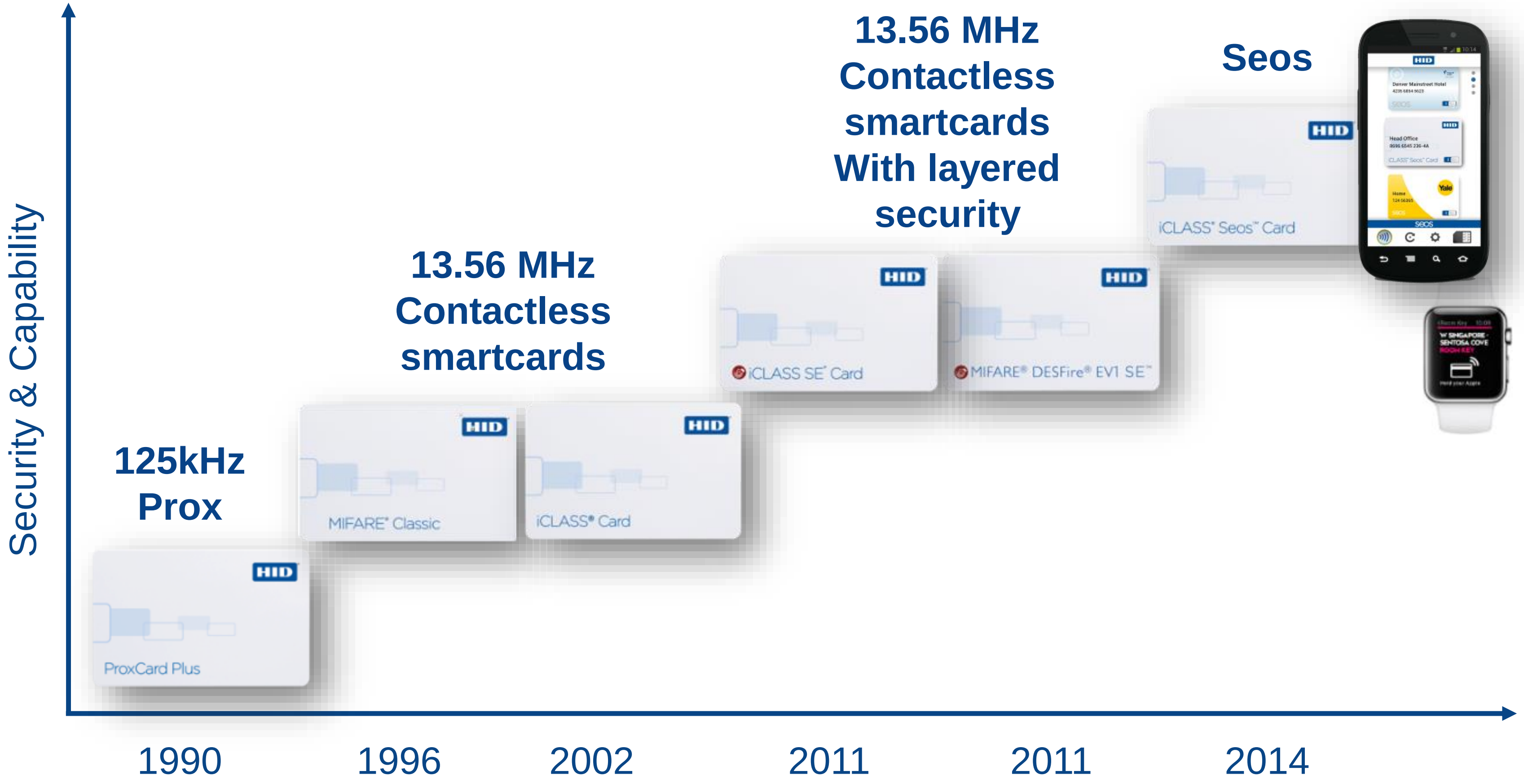
Secure Print

Time & Attendance

Cashless Vending

Windows Login

The Credential Continuum



Security & Capability

125kHz Prox

13.56 MHz Contactless smartcards

13.56 MHz Contactless smartcards With layered security

Seos

1990 1996 2002 2011 2011 2014

seos™

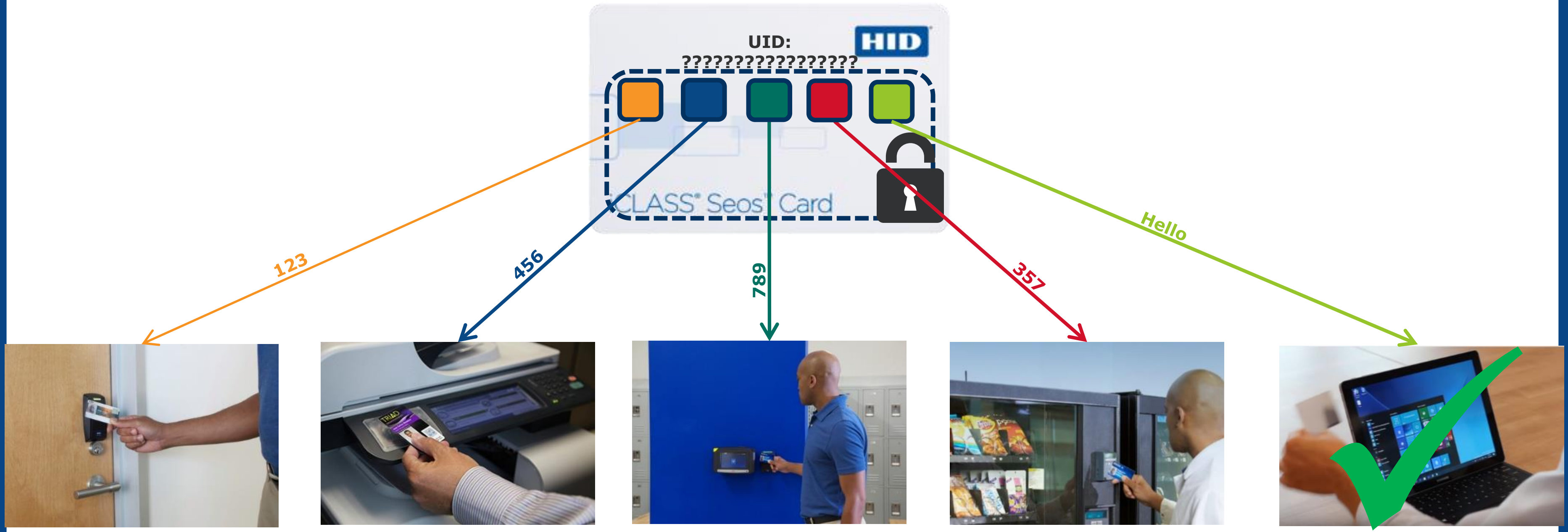
Secure Element Operating System)

Seos is the next generation of credential technology that provides the ideal mix of security and flexibility for any organization.

Thanks to highly advanced encryption and a software-based infrastructure, Seos secures trusted identities on any form factor and can be extended for applications beyond physical access control.

Selecting the Right Solution

Multi-application



Physical Access

Secure Print

Time & Attendance

Cashless Vending

Windows Login

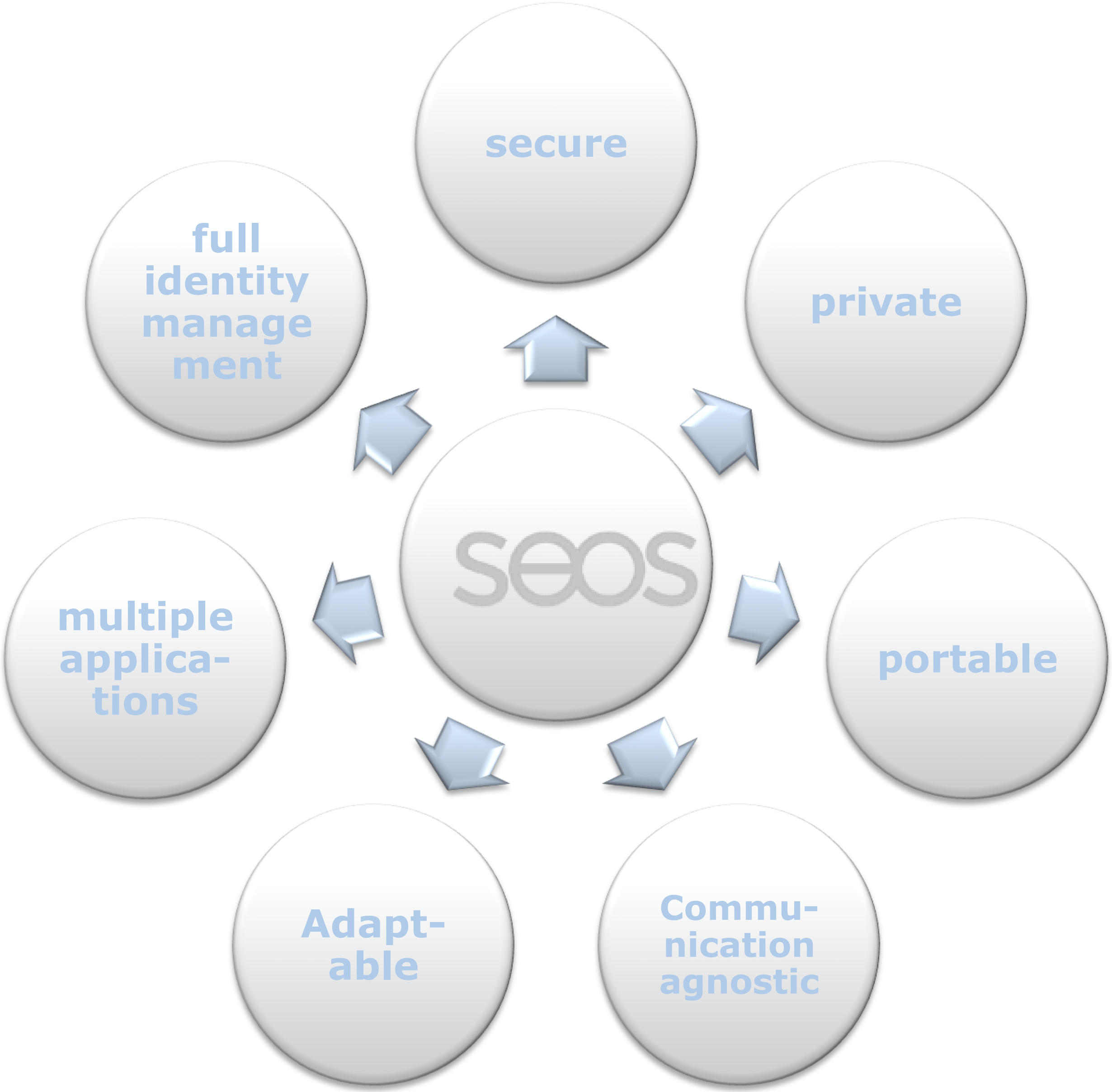
Selecting the Right Solution

More applications

Leverage technology that makes it possible to incorporate an increasing number of physical, logical, and extended applications:

- Building access
- Secure print authentication
- Time and attendance
- Cashless vending
- Tablet or computer login
- Among many more common applications

With a **truly converged credential**



seos

secure

private

portable

Communication agnostic

Adaptable

multiple applications

full identity management

In Conclusion

- As electronic access control continues to change, the method by which devices should talk to each other should also evolve
- The status quo of legacy protocols and its limitations leads to vulnerabilities and creates barriers for scale, modernization
- When upgrading, adopt a protocol that offers more security, more functionality, and more flexibility
- Create a plan to upgrade, follow best practices, and watch for potential pitfalls in the process