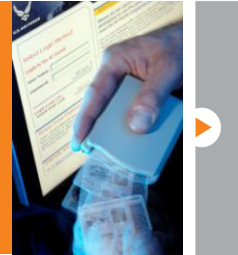


The convergence of logical and physical access control

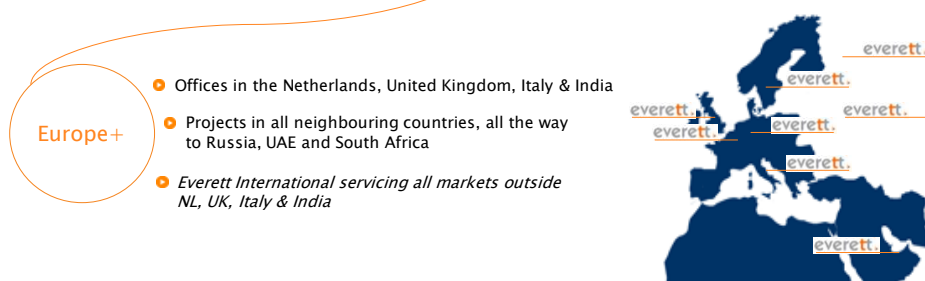
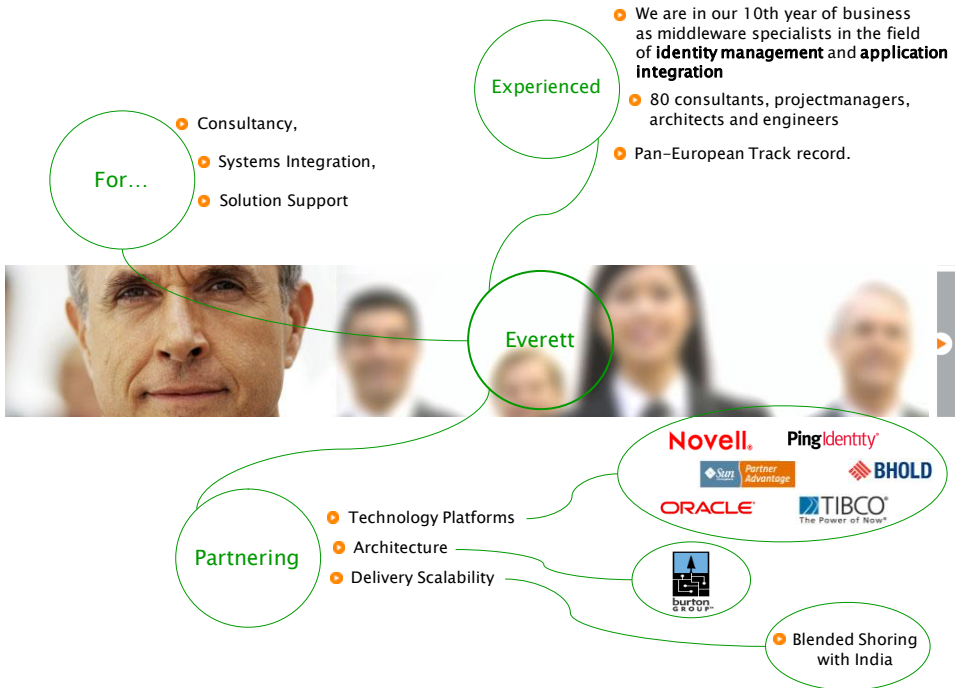
Thomas van Vooren <thomas.van.vooren at everett.nl>



www.everett.nl

Agenda

- ▶ Necessity of convergence;
- ▶ Convergence architecture;
- ▶ Benefits of convergence;
- ▶ Approach and takeaways.

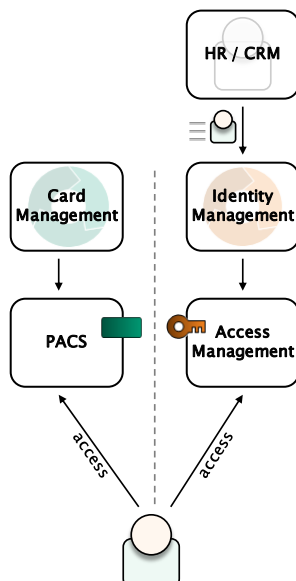


Why is convergence relevant?

- ▶ The cost of security keeps rising, across society:
 - Increasing number of services subject to access control (both logical and physical)
 - Necessity to grant access to an increasing variety of users (internal and external)
- ▶ Access control is mission critical in various industries, both logical and physical:
 - Aerospace, Finance, Public domain, High-Tech Industry, etcetera.
- ▶ Means to establish access control are expensive:
 - Smartcards, readers, access gates, IT-access management systems, administration, etcetera.
- ▶ And isolated solutions are insufficient to provide the required level of security and controlled risk:
 - Gaps in the process of granting and revocation of authorisations.
 - Incomplete coverage of risks.

5

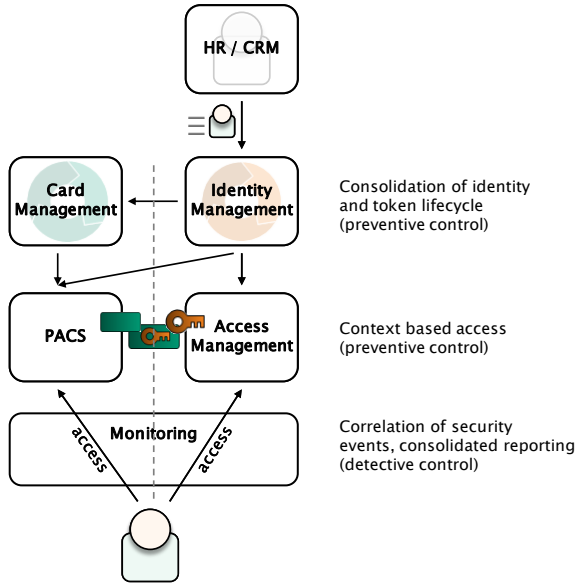
Traditional separation of logical and physical domain



- ▶ Separate administration process to manage identity and credentials;
- ▶ Various means of authentication;
- ▶ Separate security domains (not cohesive).

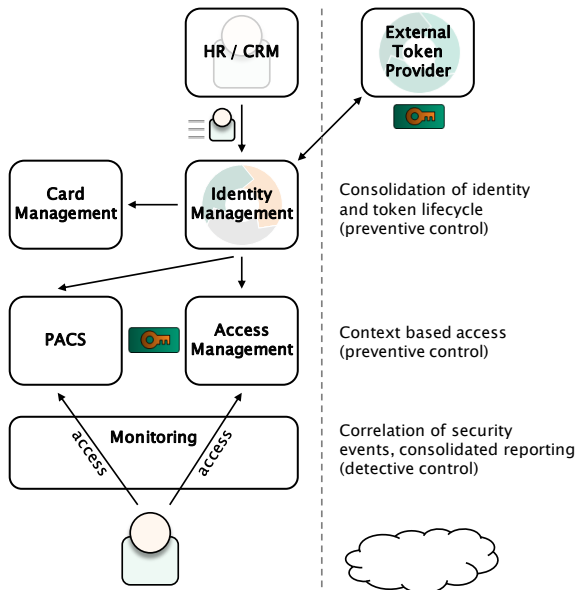
6

Convergence within the enterprise



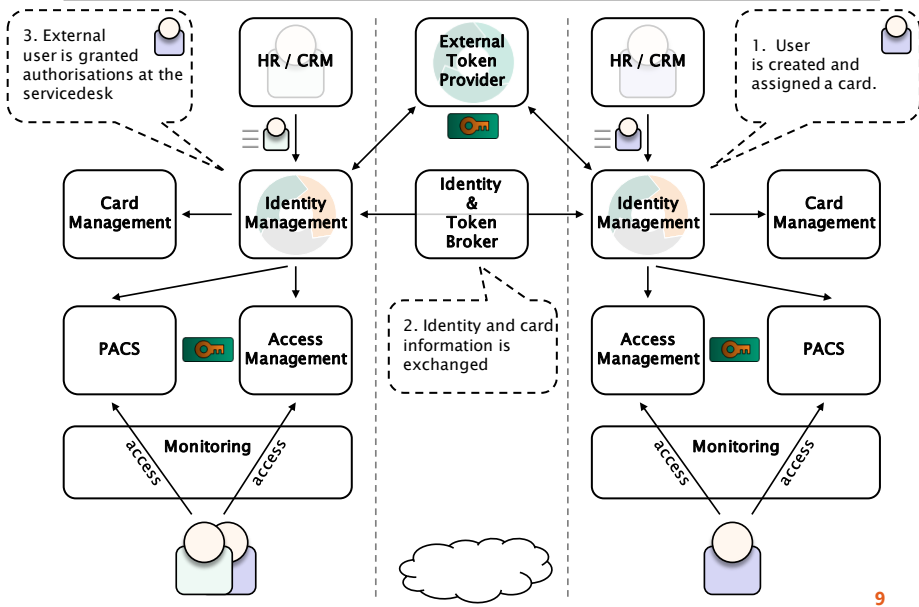
7

Convergence with an external provider



8

Cross domain convergence



Typical benefits of logical and physical convergence

- ▶ Lower cost of ownership:
 - Reduced administration cost
 - Reduced token costs
- ▶ Improved security:
 - (often) stronger authentication (2-factor)
 - Traceability
 - Context based access (e.g. logical access only on site)
- ▶ Improved compliance:
 - Consolidated auditing and reporting across physical and logical domain.
- ▶ User friendliness:
 - Same token for multiple access domains;
 - Reduced or single sign on.

The road to convergence

- ▶ The key to convergence of logical and physical access is cohesive identity and autorisation management.
- ▶ Determine architecture, solutions fit for requirements and desired benefits.
- ▶ Bring together facility management department and IT department.
- ▶ Attention to both organisation as well as technology;
 - Touches both policy and work processes across departments;
 - Interoperability card and infrastructure.



11

Questions



12