Le politiche ed i processi per la Sicurezza IT

Gestione e Monitoraggio delle utenze privilegiate per l'amministrazione dei Sistemi IT

Alfonso Ponticelli

Privileged Identity Management

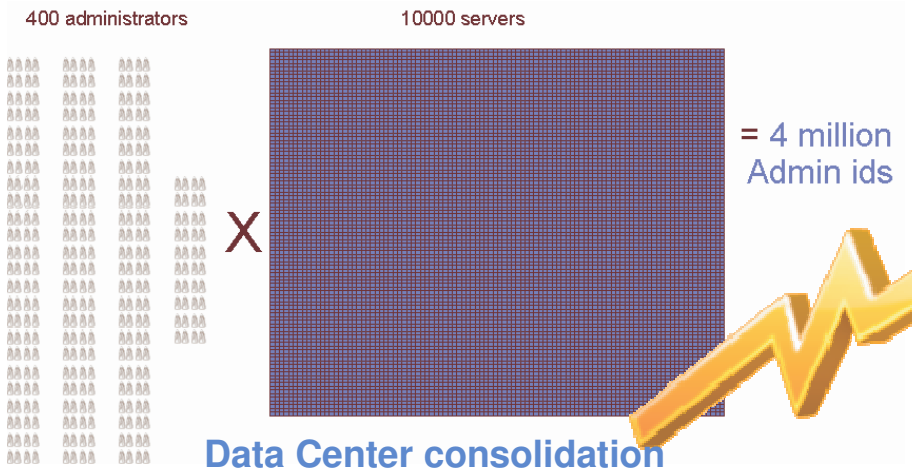
- What is a privileged identity
  - Have access to sensitive resources
  - Required by virtually all platforms although modern platforms have more capabilities for separating PIM from real user access
  - Usually shared
  - Examples:
    - Root
    - Oracle Financials Admin
    - Directory Server Admin
    - Unix File Shares Admin
    - DB2, SQL Server Admin
    - FileNet Admin
    - AD Domain Admins
    - SAP Admin
    - Security Infrastructure Admin

IT Administrators

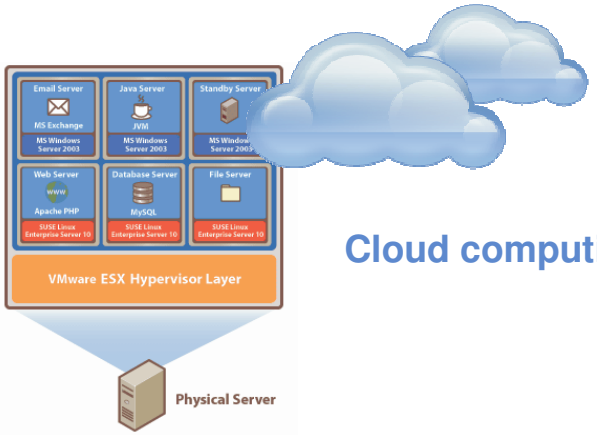
System Accounts

Business Executives

Data Center trends, Virtualization and Cloud Computing drives an exponential increase in Privileged IDs

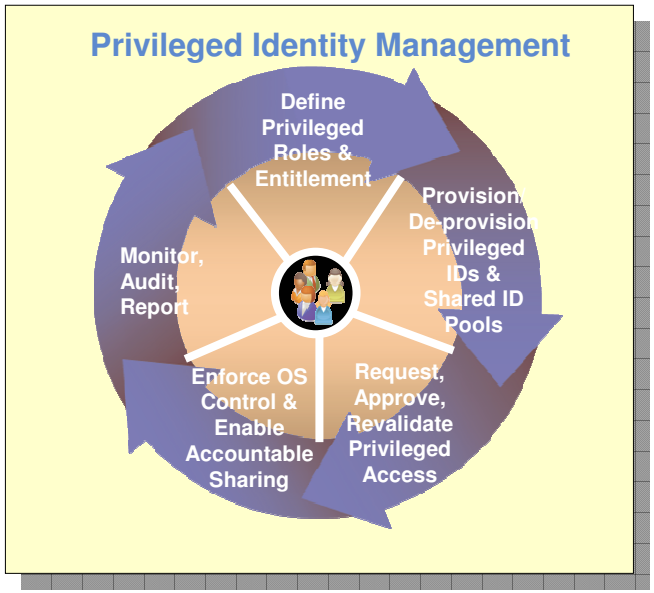


Data Center consolidation



Cloud computing

Virtualization



Problem Statement

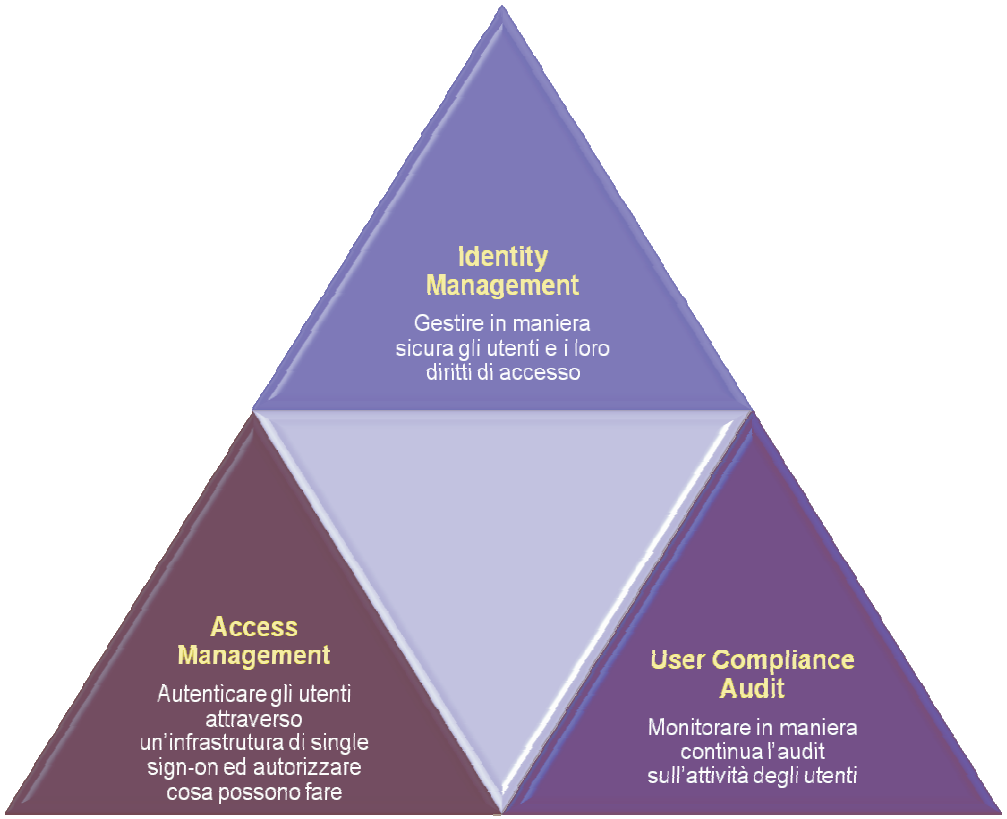
The traditional Identity Management approach requires EITHER:

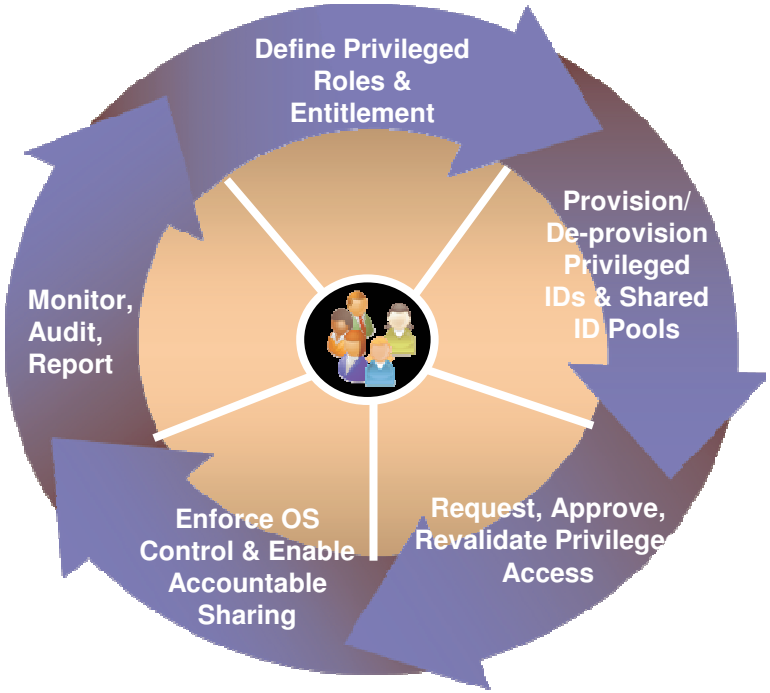
- Each administrator to have a userid on every system they administer
  - Exponential increase in privileged userids
  - Increased risk of mismanagement of privileged userids
  - Increased userid administration costs

OR

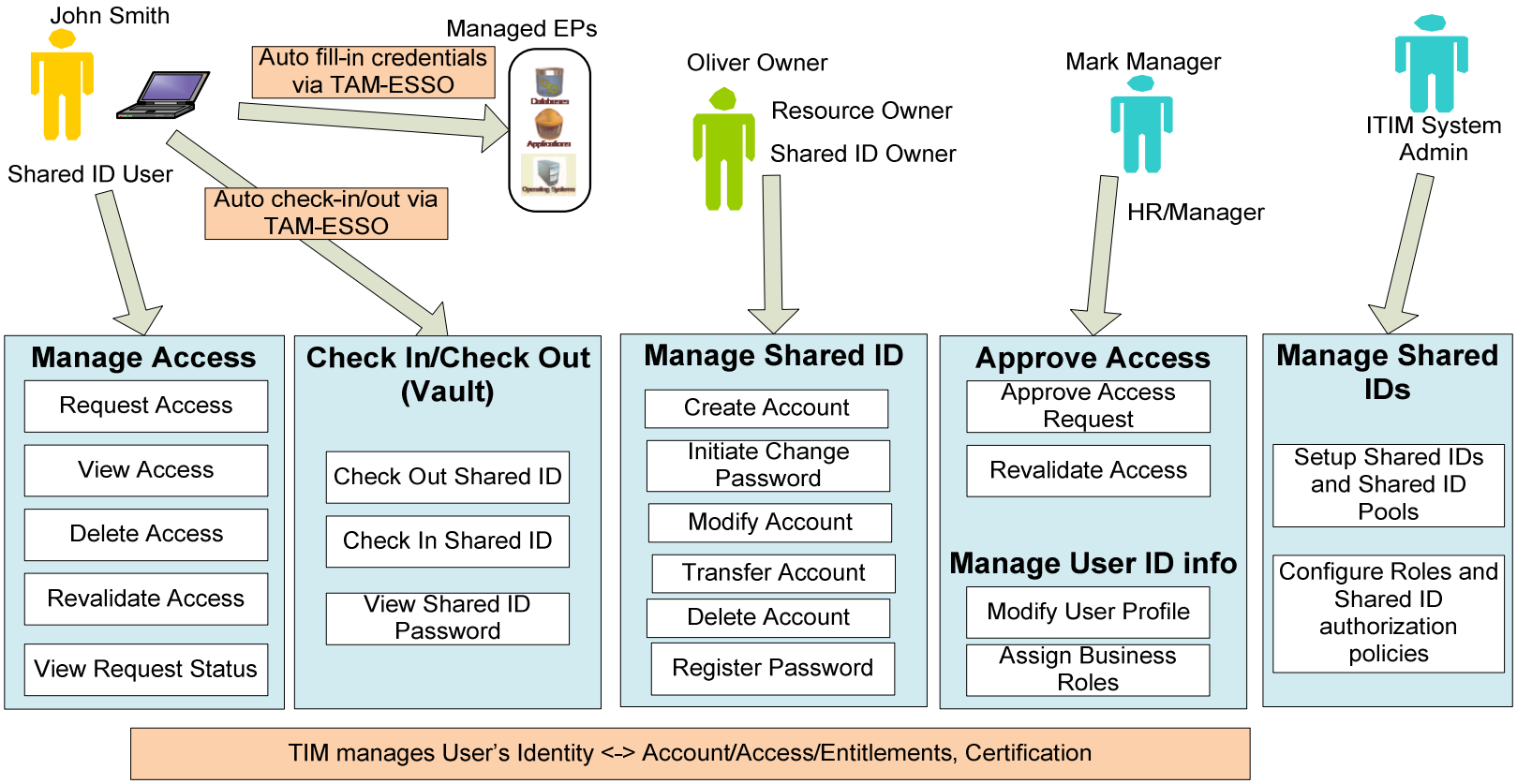
- Administrators share privileged userids
  - Risk of losing ‘accountability’
  - Issues with password management and security
  - Out of step with regulatory thinking
- Privilege Identity Management combines the best features of both approaches, without the disadvantages

Closed loop identity and access assurance throughout the identity lifecycle – from proofing a user, to issuing credentials to monitoring user activity

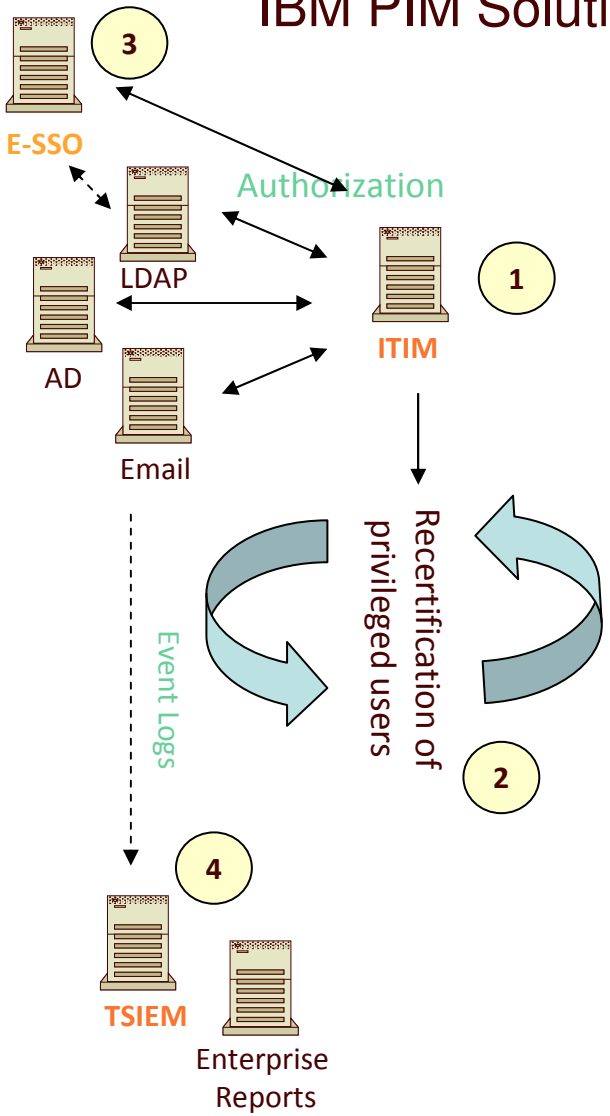




Actors for Demo



IBM PIM Solution (TIM, TAMesso and TSIEM Integration)



1
- TIM with custom module provisions privileged IDs and manages pools of shared IDs
- Shared IDs are stored in a secured data store

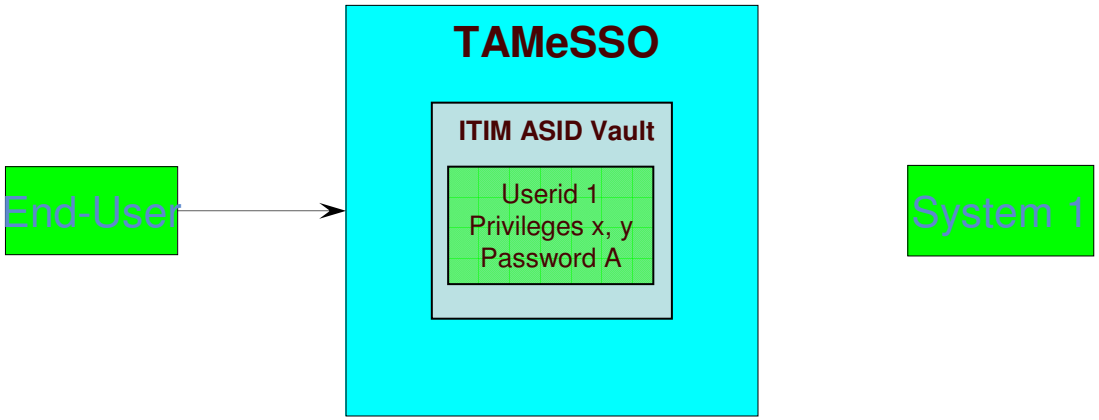
2
- Periodically recertify account authorizations through a consistent work flow.

3
- Admin logs into TAM E-SSO
- TAM E-SSO automatically checks out/in shared ID as required to ensure accountability while simplifying usage

4
- TSIEM monitors all logs for end to end tracking

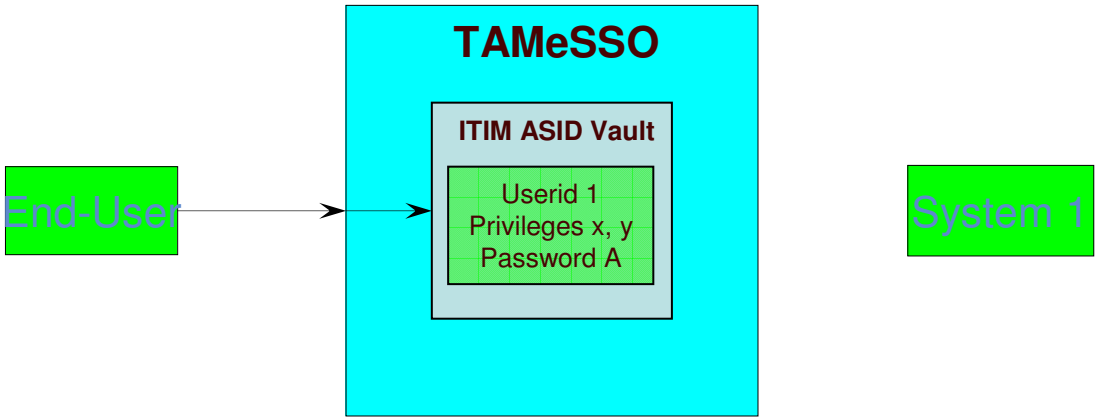
Usage – User wants to access a system

1. **End-User asks TAMeSSO for access to system 1, using his/her TAMeSSO UserID 1**



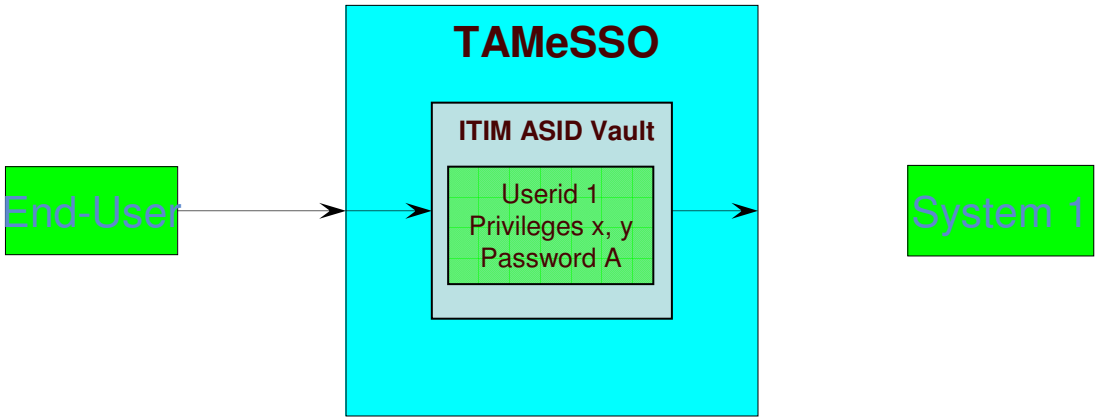
Usage – User wants to access a system

1. End-User asks TAMeSSO for access to system 1, using his/her TAMeSSO UserID 1
2. **TAMeSSO asks ITIM**



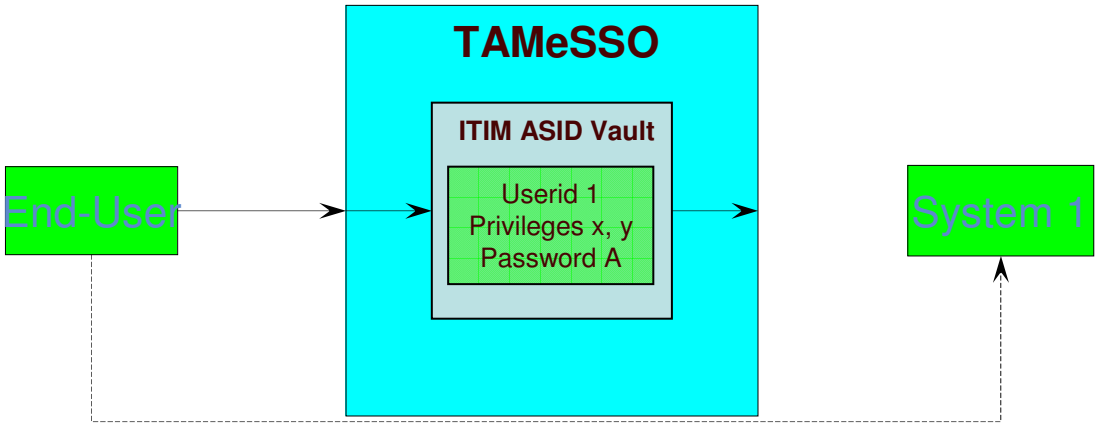
Usage – User wants to access a system

1. User asks TAMeSSO for access to system 1, using her/his TAMeSSO UserID 1
2. TAMeSSO asks ITIM
3. **ITIM gives TAMeSSO the Privileged UserID and Password**



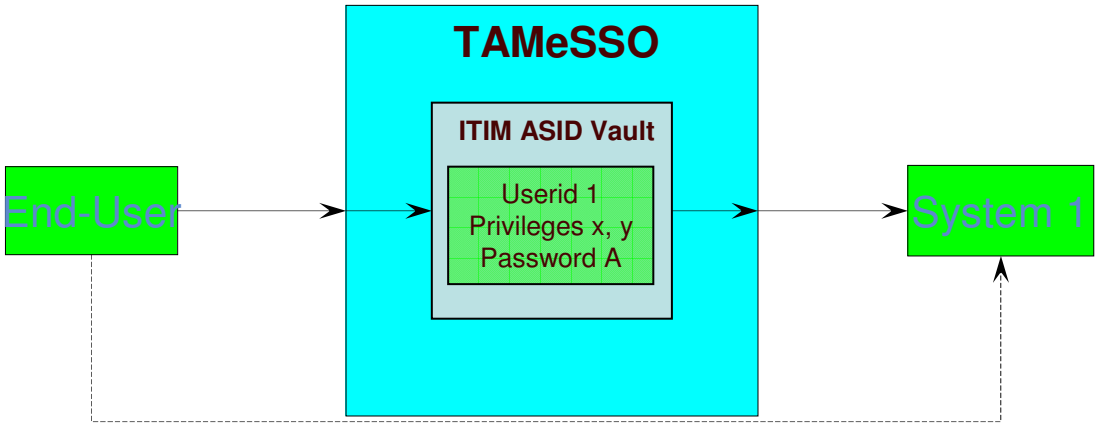
Usage – User wants to access a system

1. User asks TAMeSSO for access to system 1, using her/his TAMeSSO UserID 1
2. TAMeSSO asks ITIM
3. ITIM gives TAMeSSO the Privileged UserID1 and password
4. **End-User connects to system 1, using Privileged UserID 1**



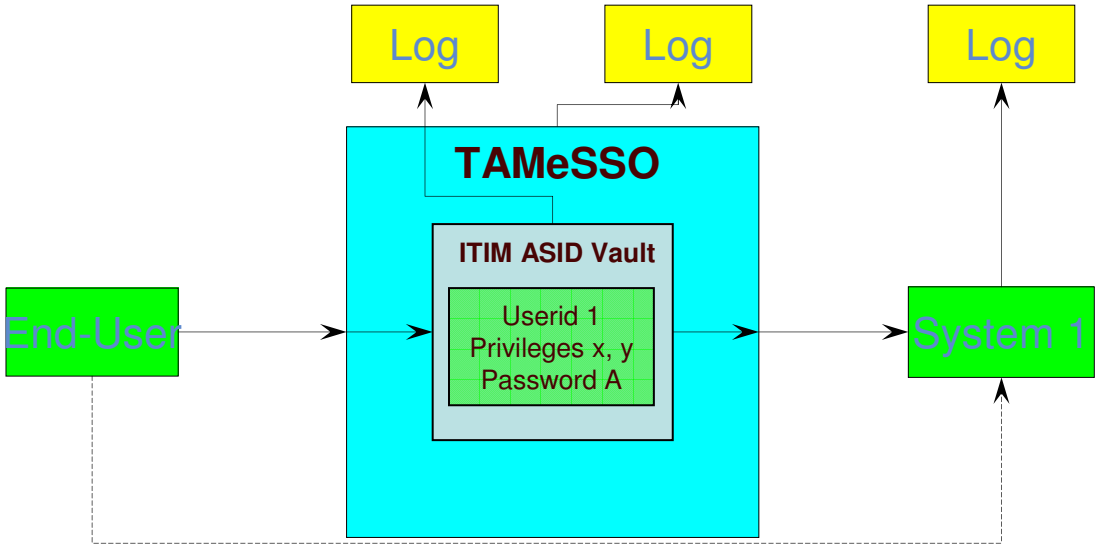
Usage – User wants to access a system

1. User asks TAMeSSO for access to system 1, using his/her TAMeSSO UserID 1
2. TAMeSSO asks ITIM
3. ITIM gives TAMeSSO the Privileged UserID 1 and password
4. User connects to system 1, using the Privileged UserID 1
5. **At logon, TAMeSSO enters the Privileged UserID1 and Password**



Usage – User wants to access a system

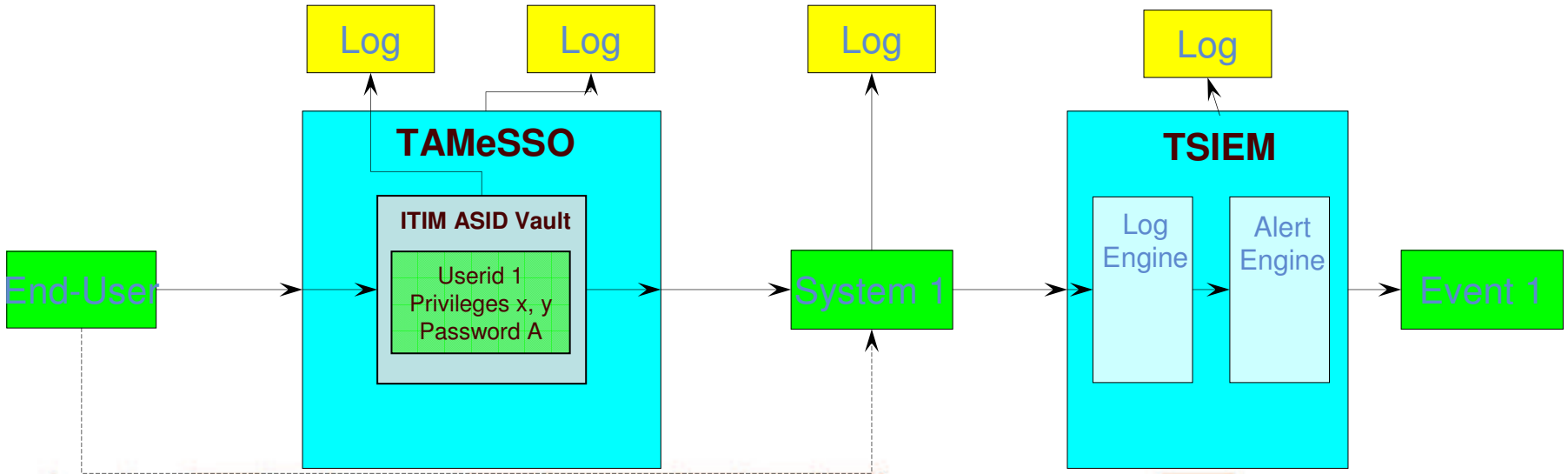
1. User asks TAMeSSO for access to system 1, using his/her TAMeSSO UserID 1
2. TAMeSSO asks ITIM
3. ITIM gives TAMeSSO the Privileged UserID 1 and Password
4. User connects to system 1, using the Privileged UserID 1
5. At logon, TAMeSSO enters the Privileged UserID 1 and Password
6. **All stages of the process are logged independently**



Usage – User wants to access a system

1. User asks TAMeSSO for access to system 1, using his/her TAMeSSO UserID 1
2. TAMeSSO asks ITIM
3. ITIM gives TAMeSSO the Privileged UserID 1 and Password
4. User connects to system 1, using the Privileged UserID 1
5. At logon, TAMeSSO enters the Privileged UserID 1 and Password
6. All stages of the process are logged independently
7. **TSIEM available for Privilege Monitoring if required**

End-to-end id management, accountability, monitoring, password secrecy



Benefits - Operational

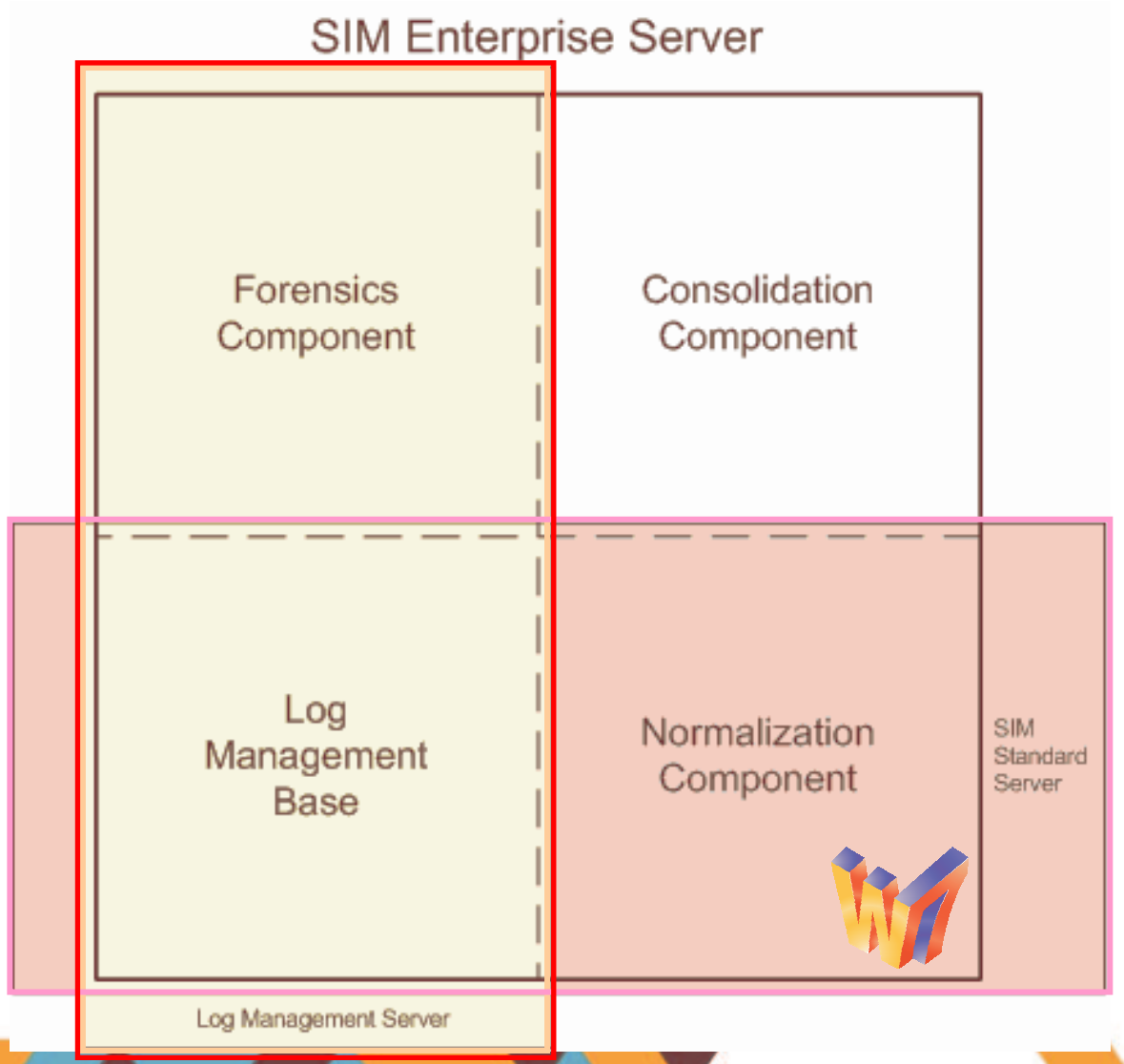
- Reduces the number of ‘unused’ privileged ids
- Reduces the number of shared ids
- Provides a central, auditable control point for ids
- Can be implemented immediately without complex prerequisites
- Modular design, independent components
- Provides a clear path to GDF implementation:
  - Create the pooled userids for GDF administrators
  - Administrators stop using individual userids
  - Identify and disable unused individual userids

Benefits - Innovation

- Moves away from two obsolete concepts:
  - "Everyone has a userid on every system, all the time, just in case"
  - "Everyone shares access to a single userid for ease of administration"

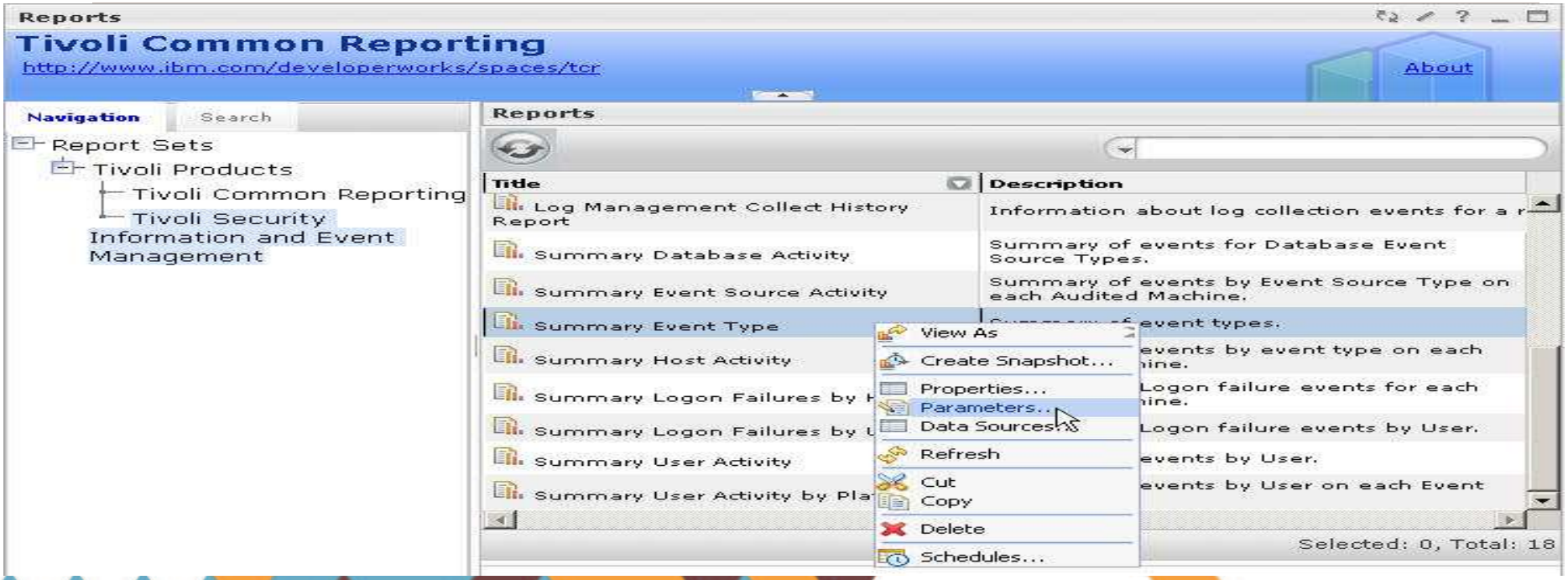
- We are moving to a new concept
  - "A user gets an individual userid on a system – but only…
    - If they need it
    - When they need it
    - For only as long as they need it"

Audit & Compliance - TSIEM 2.0 and his Components



TSIEM 2.0 Log Management server features

- Reliable and scalable log collection and archiving
- Flexible integration, able to collect any type of log located on any type of machine in a tcp/ip network.
- Out-of-the-box log management reports
- Out-of-the-box best practice log analysis reports.
- Customizable search tool for advanced log analysis.



Features: reliable and scalable

- Reliable Log collection using TSIEM guaranteed log collection mechanism.
  - Encrypted data transfer (3-DES)
  - Secure channel (RSA)
  - Compression rate 0.15
- Secure Log archive
  - Log archive storage on IBM Storage Solution ensures log integrity
  - Log Manager continuity report monitors quality of the log archive
- Scalable Log Management servers
  - High performance syslog/SNMP collector capable of processing up to 30.000 events per second
  - One Log Management server manages around 5000 event sources
  - One Log Management server collects and archives up to 180 GB per day. (equal around 200.000.000 events per day)
  - Once a log has been archived its contents is always available for log analysis. The log can be exported from the archive to save disk space.

Grazie