PATECCO
dynamic identity systems.

PATECCO BEST PRACTICES IN IDENTITY & ACCESS MANAGEMENT

- Identity & Access Management
- Public Key Infrastructure
- Privileged Account Management
- Microsoft Active Directory Integration

Table of Contents:

About PATECCO

PATECCO is an international managed services company with a focus on Identity and Access Management, Cloud Access Control, Security, Information and Event management, Public Key Infrastructure and Privileged Account Management. PATECCO's strategy and unique technology help customers to close security gaps and leverage standards and guidelines for an easy application onboarding into IAM systems.

- PATECCO is independent, no software reseller, strong cooperation with vendors and product teams.

PATECCO enables organisations to:

- **Simplify** user password management across information systems
- **Strengthen** security and compliance
- **Manage** users' identities and access rights
- **Control** the lifecycle of employee’s identities and access rights
- **Automate** account and rights provisioning across all apps
- **Audit** information systems and manage access rights

PATECCO ensures:

- **Global capability:** We design, deploy, manage and monitor for clients of all sizes and industries around the world.
- **Security:** We secure, accelerate and improve the broad view of IT processes in a heterogeneous IT landscape
- **Compliance**: We help Organizations Meet Compliance Requirements
- **Flexibility**: We offer 3 levels of support for managed services: Remote, Onsite Support for Business Critical Issues, and Onsite on Demand
- **Industry expertise**: We invest in robust training programs to ensure that our consulting and managed services professionals deliver value, protect your organization, and stay abreast of global trends and best practices.
- **Long-term customer retention**: It is based on our core values like trust, productivity and engagement
- **Fixed-price projects:** Based on defined scope

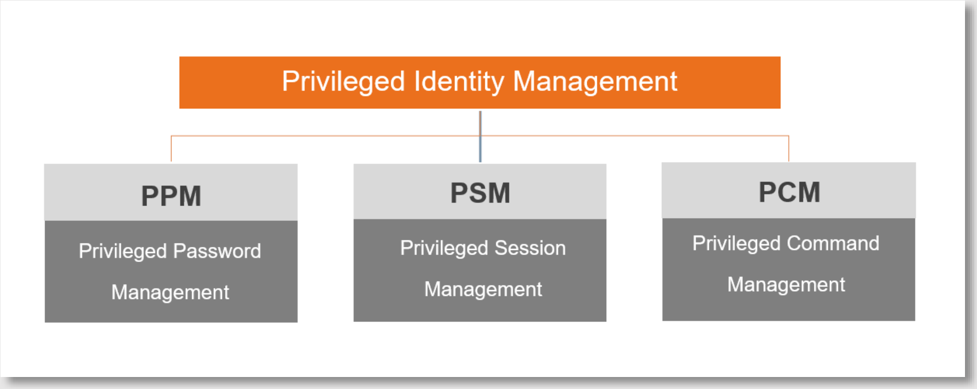
Protect Your Business with Privileged Account Management

Privileged Account Management (PAM) focuses on the specific requirements of privileged user accounts in a company's IT infrastructure. PAM is used as an information security and governance tool to support companies in complying with legal and regulatory compliance regulations. It also helps to prevent internal data misuse through the use of privileged accounts. If this does not work, PAM should be used to detect and trace this abuse.

Typical regulations for dealing with privileged identities and users, as well as accounts, can be found in standards, regulations and laws for specific industries.

PATECCO PAM Projects

- Demonstrate PAM capabilities allowing privileged users to have efficient and secure access to the systems they manage
- Ensure that audit and compliance requirements are met
- Offer secure and streamlined way to authorize and monitor all privileged users for all relevant systems
- Implement privacy policies adherent to GDPR compliance


Privileged Identity Management
PPM
Privileged Password Management
PSM
Privileged Session Management
PCM
Privileged Command Management

- **Privileged Password Management (PPM)** enables secure (encrypted) storage, release, control and change control of privileged passwords in a heterogeneous environment of systems and applications. A Privileged Password Manager also replaces embedded passwords that are encoded in scripts, procedures and programs.

- **Privileged Session Management (PSM)** provides control, monitoring and recording of sessions of high-risk users, including administrators and, for example, remote support providers.

  - Who (user name / ID) checked out or checked in ID?
  - What role was requested and used and what was done with it (Audit Trail / Session Recording)?
  - When (timestamp) was the privileged ID checked in or checked out?
  - On which (application or system) was the privileged ID used?
  - Where (IP address) was the check-out requested from?
  - Other factors, e.g. command detection

- **Privileged Command Management (PCM)** provides the ability to granularly delegate user access to specific programs, tasks and commands across multiple platforms. It provides command control capabilities with the ability to delegate privileges (sometimes called "elevation").

PAM implementation process

For the past several years, PATECCO developed high skills in implementing PAM solutions, describing and designing necessary processes, and connecting systems to these solutions. Its IT consulting team can offer best practices in the following functional PAM subsets:

1. Identity Consolidation

- Consolidate UNIX, Linux, LDAP identities under a single unique ID in Active Directory for centralized identity, role, and privilege management and Kerberos-based authentication
- Deleting or disabling as many privileged accounts as possible to reduce the attack surface

2. Privileged Access Request

- Establishing a solution (tool) that supports workflow-based privileged access request across both SUPM and SAPM components for stronger security, governance, and compliance

3. Super User Privilege Management (SUPM)

- Minimizing the number of shared accounts. Reduce/disable the number of privileged accounts. Use of host-based SUPM for least privilege login with unique ID and explicit privilege elevation wherever possible.

4. Shared Account Password Management (SAPM)

- Data breach mitigation is most effective when reducing the attack surface — reducing the number of privileged accounts as close to zero as possible and only using SAPM for emergency login scenarios such as “break glass”.

5. Application to Application Password Management (AAPM)

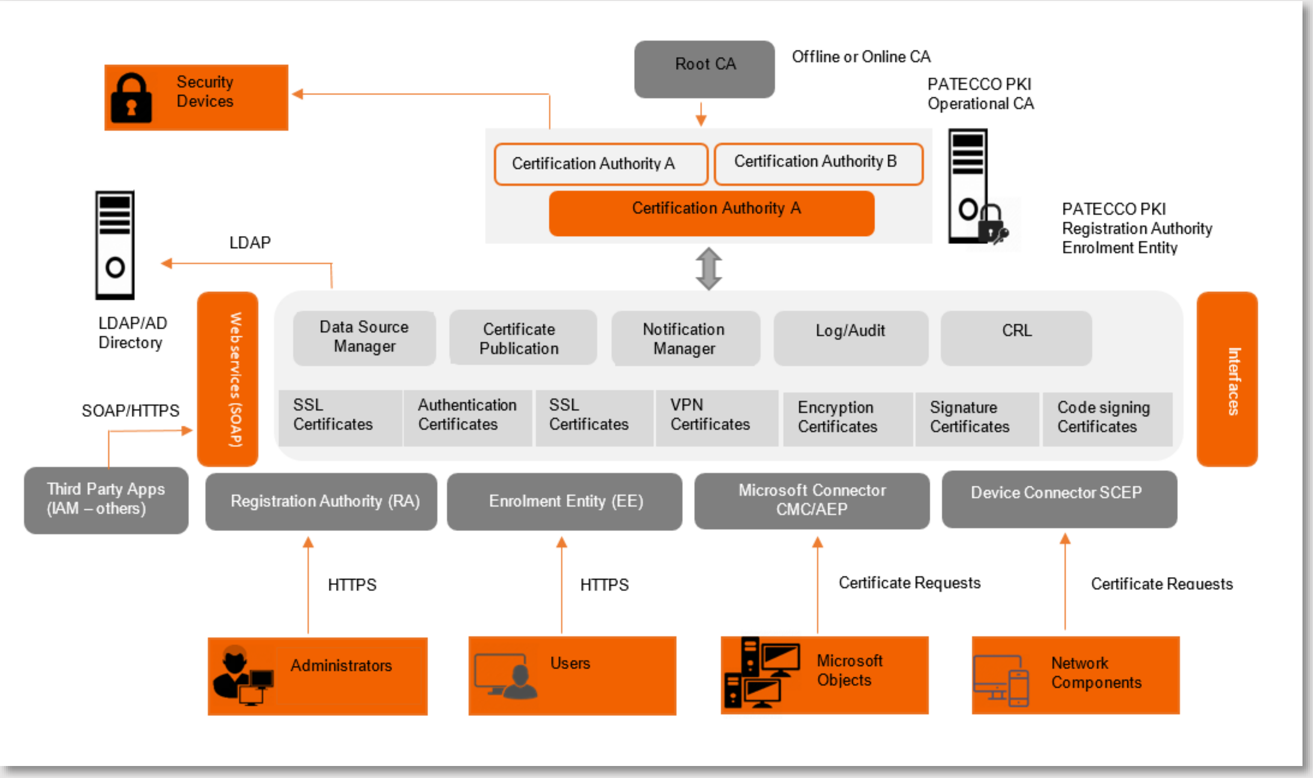
- Replacing plain text passwords embedded in scripts with an API call to a company’s SAPM service for better security and reduced IT administrative overhead.

Building Public Key Infrastructure for Stronger User Verification and Identification

Securing the keys and certificates that govern machine identities is becoming much more challenging. Not migrating your PKI to current standards could leave you vulnerable in multiple areas due to misconfiguration, weakened cryptographic configuration, expiration or outdated PKI design and architecture. Weakened PKI can degrade the trust associated with digital certificates and leave your organization prone to fraudulent certificate usage.

PATECCO prevents the problem by PKI migration and automation which simplify complex operations, maintain security assurance, and facilitate future projects and growth.

The Germany - based company is a leading provider of trusted identity and security solutions enabling businesses and large enterprises around the world to secure online communications, manage millions of verified identities and automate authentication and encryption.



PATECCO PKI Architecture

PATECCO’s PKI Capabilities

- PATECCO uses Public Key Infrastructure (PKI) as an effective method for implementing strong multi-factor authentication and to meet security compliance regulations
- PATECCO finds a great way for assigning digital identities for all employees and machines, allowing for secure access to data, networks and physical locations.
- PATECCO can implement PKI in the following high-security scenarios - S/MIME, Data encryption, Code signing, Expiring User/Server certificates, Expiring CRLs, Certificate automation and delivery, VPN/Direct Access.
- PATECCO provides secure **PKI Migration** to new environment (following Microsoft baseline security rules) and **PKI Automation** (PowerShell scripting automation of S/MIME user certificates).

PKI Migration

- During the PKI migration, PATECCO ensures that the old certificates are expired/revoked and new ones are issued within the update PKI environment. Following Microsoft baseline security rules, it has the ability to seamlessly migrate to a newly-deployed PKI without user or server downtime.

Key Benefits

- Provided consultants with years of PKI experience and knowledge of various approaches
- Protected internal infrastructure and efficient management of employee life-cycle.
- Saved valuable IT resources and reduced risk of expired certificates.
- Assured compatibility and interoperability.

PKI Automation

- PATECCO uses techniques to automate the method of recovering mail encryption certificates, S/MIME. There is an automation of the recovery of certificates, of SMIME certificates and management of the process via FIM or MIM certificate Management Services.

- PKI Automation helps deliver on the promises of PKI and the goals of your IT strategy.

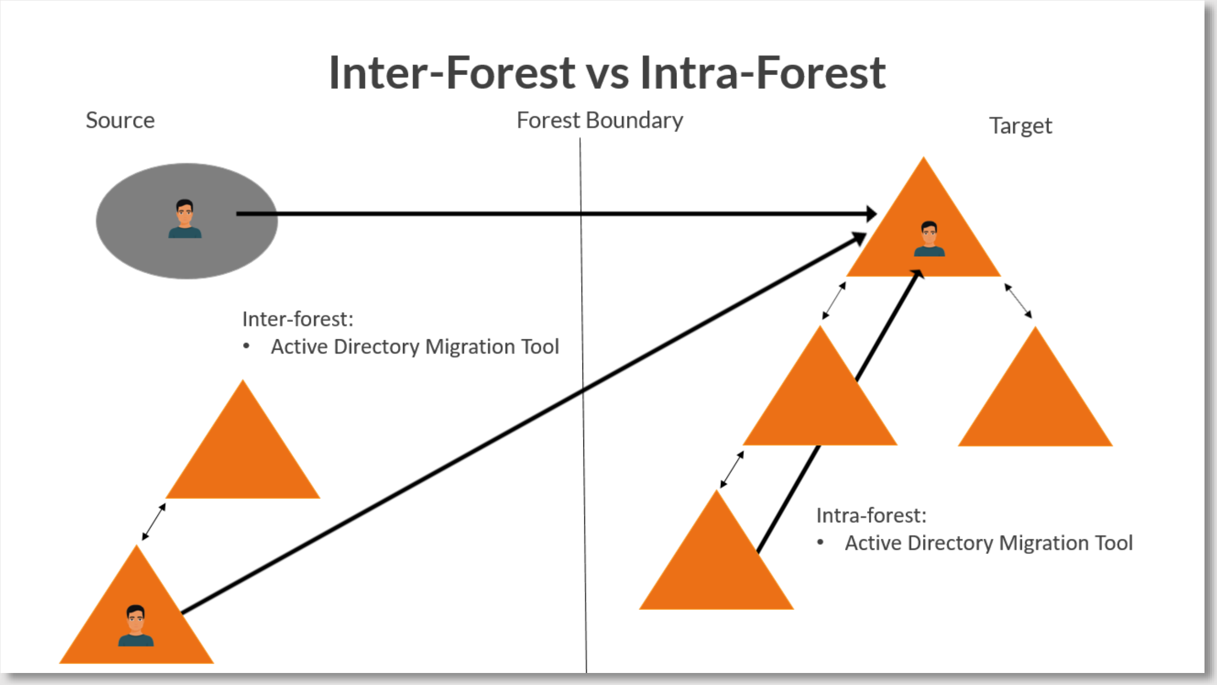
Key Benefits

- Automates your PKI Security to reduce risks to your PKI Infrastructure
- Ensures that the correct certificate is always requested and issued using the correct template and parameters.
- Ensures that all endpoints requiring that new certificate being installed are immediately addressed.
- Provides the strongest levels of confidentiality and security for electronic communications.

Key advantages of PATECCO PKI Management

- Bringing experience and expertise in using PKI and S/MIME technologies and applying them towards solving cybersecurity problems
- Ensuring comprehensive security, operational efficiency, and business continuity
- Automating certificate requests and renewals
- Continuous monitoring of keys and certificates for anomalies
- Rapid replacement of compromised keys and certificates
- Enforcing key and certificate security policies to maintain compliance

Changes in companies are normal. Sometimes they merge with other companies to sell or buy parts of business. If they set up subsidiaries they have a change, as well. Merger and Carve-Out projects transform the company into a new organizational structure.


Inter-Forest vs Intra-Forest
Source
Forest Boundary
Target
Inter-forest:
• Active Directory Migration Tool
Intra-forest:
• Active Directory Migration Tool

Older Active Directories are built with a lot of self-made scripts. To find a consultant who can handle this is not easy. If you have a new, clean infrastructure, each Microsoft administrator can support it and that reduces the costs of administration.

Security is currently a very important point. It is easier to include new security solutions during the Active Directory migration or in a structure which is like Microsoft's best practices.

Benefits of using Active Directory Services

- Highly secure: it has policies and permissions for security at different levels
- Objects can be located anywhere physically yet access the domain/network's resources securely

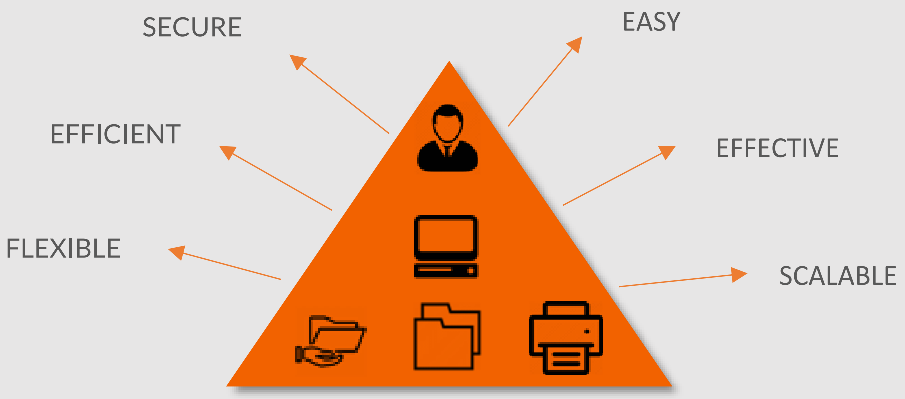
- Easily Scalable, Highly Flexible, Readily Extensible: Millions of users can be added to a single domain
- Easy, Efficient search mechanism to locate an object
- Centralized Storage -for users, departments which makes Back Up and Restore Efficient, Fast and Easy
- Efficient and Effective management of services
- Enable Single Sign-on (SSO) like log on script
- Centralized Auditing: makes it easier to track all the operations

Who can use Active Directory Services?

- Organisations that have a network setup
- Organisations which require 24/7 uptime
- Organisations where the number of users, computers or resources will keep changing
- Organisations where INFORNATION/DATA SECURITY is vital
- Organisations that operate in multiple locations

Key advantage of Active Directory Services

- Cost effective management and control mechanism to control all the objects, resources and information in an organisation/network.


SECURE
EASY
EFFICIENT
EFFECTIVE
FLEXIBLE
SCALABLE