

The Audit Portal.

primeid DISCOVER

Enhanced security through centralized, cross-system auditing of digital identities.



primeid DISCOVER connects and audits digital identities from different IT systems across an entire IT infrastructure, such as directory services, public key infrastructures (PKIs), credential management, or mobile device management systems. Identity information matching and consistency checks reveal potential inconsistencies and security risks between interdependent systems. Additionally, cross-system auditing can be integrated into the information security system (ISMS).

DISCOVERING CERTIFICATES ON MOBILE DEVICES

Certificates for mobile devices are typically obtained from a certification authority using the Simplified Certified Enrollment Protocol (SCEP). A mobile device management (MDM) system then distributes the certificates to the individual devices. Usually, it is not recorded, which certificate is installed on which device. primeid DISCOVER overcomes this weakness by connecting certificates and devices and revealing interrelationships between them.

DETECTION OF INCONSISTENCIES ACROSS SYSTEMS

primeid DISCOVER connects and matches identity data from users, devices, and certificates of different, interrelated IT systems. This enables inconsistencies between individual systems to be detected quickly. Additionally, a chronological change log supports fast and easy troubleshooting.

EXPIRY NOTIFICATIONS

primeid DISCOVER provides notifications regarding upcoming or pending certificate expiry. This allows for the reliable and timely renewal of certificates, preventing any system downtime or pause in production.

PUBLIC



cryptas.com . prime-sign.com . cryptoshop.com

we protect identities.

Vienna | Graz | Düsseldorf | Stockholm

The Audit Portal.

primeid DISCOVER

Enhanced security through centralized, cross-system auditing of digital identities.

To establish trust in the entirety of all IT systems across an IT infrastructure, IT security officers must be able to associate every certificate with a user and/or device, and the respective purpose or key usage at any time. This is complicated by the fact that many individual IT systems are typically used to create or manage user, device, and certificate data. These systems are in constant exchange with each other but are usually managed independently. As a result errors and inconsistencies can hardly be avoided in the long run. To ensure the trustworthiness of digital identities across all IT systems, a supervisory authority is needed to audit and consolidate individual systems and identify inconsistencies between them.

OUR SOLUTION

primeid DISCOVER creates a central and integral database by aggregating data from users, devices, and certificates from the individual systems across an entire IT infrastructure. Connecting and matching data allows inconsistencies and errors to be detected and promptly fixed. For example, certificates may be found which still exist but

are no longer manageable due to replaced devices. Similarly, smart cards may be identified that still have a valid certificate, but whose users are no longer with the organization, and therefore no longer in the directory.

BENEFITS

- ☞ Transparency of all systems that are relevant to IT security
- ☞ Central and integral database
- ☞ Reporting & messaging
- ☞ Identification of inconsistencies and resulting vulnerabilities
- ☞ Intelligent, cross-system gathering of security-relevant information
- ☞ Complex system dependencies, including object history, at a glance
- ☞ Simple installation and maintenance
- ☞ Plug-in system for easy extensibility
- ☞ Easy operation

FEATURES

- + LDAP interfaces
- + Interfaces with PKIs of different vendors
- + Interfaces with mobile device management systems
- + Custom interfaces on demand
- + HTTPS / REST interfaces
- + LDAP-based authentication of security officers (users of primeid DISCOVER)

CONTACT

Any questions?
Need more information?
Contact us under:

office@cryptas.com
T: +43 (1) 3 555 3 - 0

