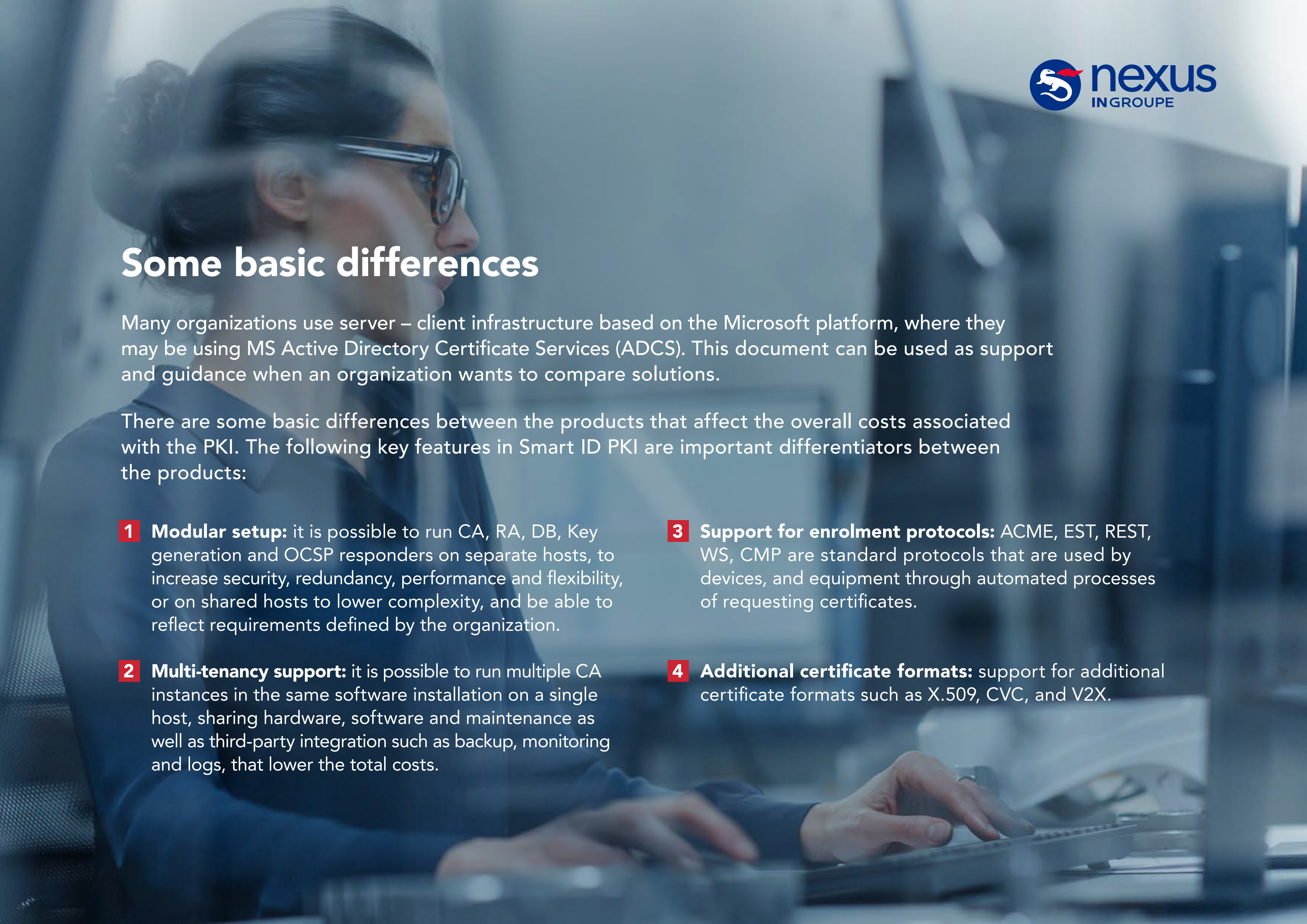
Evaluating PKI Platforms?

COMPARISON: Nexus Smart ID PKI Platform
vs Microsoft Active Directory Certificate Services

nexusgroup.com



Some basic differences

Many organizations use server – client infrastructure based on the Microsoft platform, where they may be using MS Active Directory Certificate Services (ADCS). This document can be used as support and guidance when an organization wants to compare solutions.

There are some basic differences between the products that affect the overall costs associated with the PKI. The following key features in Smart ID PKI are important differentiators between the products:

1. **Modular setup:** it is possible to run CA, RA, DB, Key generation and OCSP responders on separate hosts, to increase security, redundancy, performance and flexibility, or on shared hosts to lower complexity, and be able to reflect requirements defined by the organization.

2. **Multi-tenancy support:** it is possible to run multiple CA instances in the same software installation on a single host, sharing hardware, software and maintenance as well as third-party integration such as backup, monitoring and logs, that lower the total costs.

3. **Support for enrolment protocols:** ACME, EST, REST, WS, CMP are standard protocols that are used by devices, and equipment through automated processes of requesting certificates.

4. **Additional certificate formats:** support for additional certificate formats such as X.509, CVC, and V2X.

Additional examples of differentiators

Topic	Nexus USP	Comparison Microsoft
Economical / efficiency	Low administration and maintenance work due to low complexity and low number of servers	Require higher administration and maintenance due to more deployed hardware, software and functions
	Lean infrastructure due to less hardware and software when multiple CAs are sharing hardware, software and database	Require dedicated servers or VM per CA including databases
	PKI-software supports additional use-cases and different types of certificates	Microsoft ADCS supports use-cases within their own platform
	Support for multiple software platforms such as Linux	Microsoft ADCS mainly supports use-cases within their own software platform
Multi-tenant solution	Reducing hardware, software and operational costs running multiple CAs in same installation	Each ADCS CA needs additional hardware / VM and software installation.
Security / compliance	Increased security due to support of physical separation between RA, CA, DB, OCSP and HSMs	RA and CA are running within the same software installation
	Easier audit due to low complexity, limited user access and 4-eyes principal, well defined interfaces, certified software	Harder to protect the Microsoft ADCS regarding its functions, no 4-eyes principal functions to be enforced

Topic	Nexus USP	Comparison Microsoft
Secure platform	Smart ID PKI and OCSP Responder are Common Criteria EAL 4+ certified with functions as 4-eyes principal and signed logs	No EAL 4+ certification or dual control
Enable automation	Limiting human errors or simplifying tasks to lower administrative work and mitigate risk through automated renewal processes	Less automation is available with less support for external protocols
Multiple enrolment protocols	Multiple enrolment protocols supporting automation and use-cases outside the Microsoft platform	Microsoft only supports SCEP-NDES as external protocol
Multiple types of certificate profiles	Different certificate profiles supporting CVC, Tachographs, V2X, OpenPGP, WTLS certificates, used in different use-cases	Only support for standard X.509 certificates within the Microsoft platform use-case
High availability	Can be configured to run as active-active, active-passive and as single or double cluster	MS ADCS only supports active-passive setup
Certificate validation	Enables standalone OCSP responders adding security, performance, limiting inbound communication to CA	MS ADCS provides limited functionality
Registration interface	The registration interface can be customized through its workflow engine	MS ADCS require external CMS software

How (and why) to migrate to Nexus's certificate authority (CA) software

Many organizations feel stranded after their CA software vendors have discontinued their products. *"We have created a smooth solution for migrating to our time-tested CA software Nexus Smart ID PKI. It is also well-suited for those who want to switch from Microsoft's ADCS or consolidate their different CA systems,"* says Martin Furuhed, product manager for Smart ID PKI at Nexus.

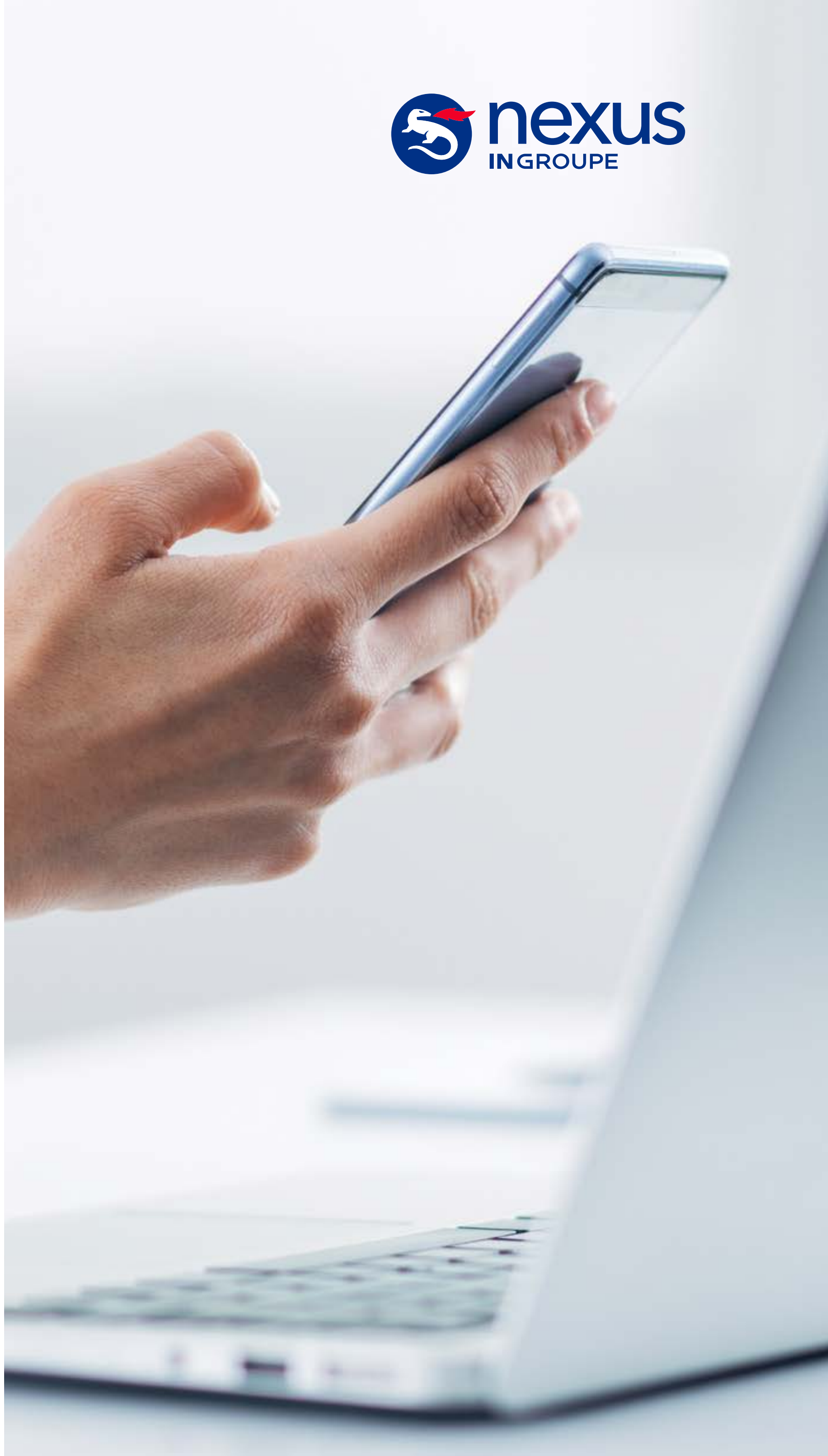
Smart ID PKI is a flexible, multi-tenant public key infrastructure (PKI) platform, trusted by a wide range of organizations including enterprises, state departments, defence organizations and service providers.

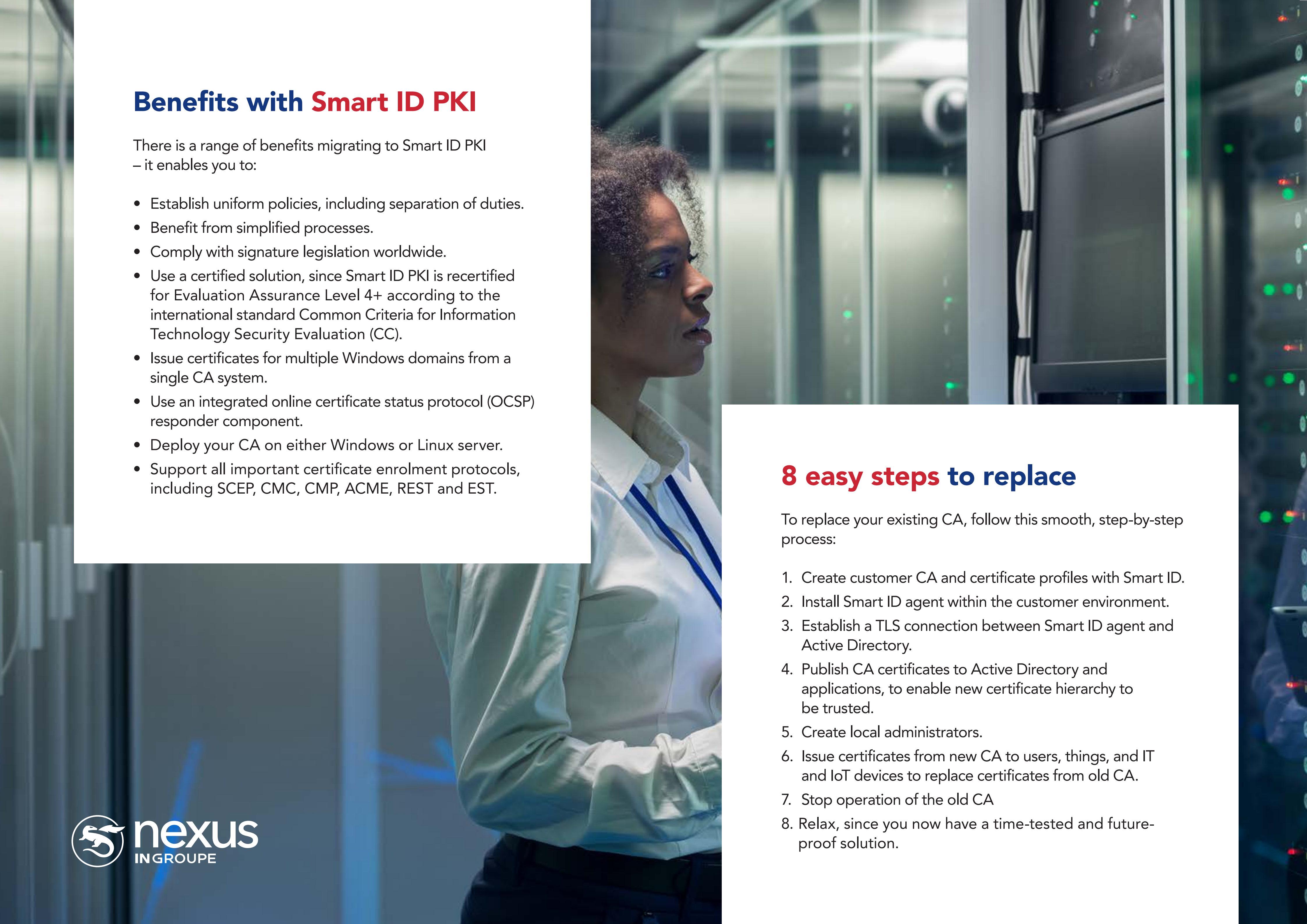
"Since Smart ID PKI is scalable, it's equally well-suited for a small organization with an internal enterprise identity deployment as it is for a service provider with hundreds of hosted CAs – it can efficiently issue and manage millions of certificates. Organizations such as Volkswagen Group, Nordea, Euroclear and Bundesdruckerei have been relying on our software for many years," he further elaborates.

A future-proof solution
Nexus has had great success with Smart ID PKI ever since its launch in 1996, and is investing heavily in it, Furuhed explains.

"We refine it continually to meet new customer needs and to support new standards, so Smart ID PKI is a safe choice for those needing a replacement for a discontinued CA software, such as RSA Digital Certificate Solutions. It is also one of the very best choices on the market for those who want a more competent CA solution than Microsoft's Active Directory Certificate Services (ADCS)," he adds.

Some organizations use several different CA systems, due to historical reasons or different requirements and issuing policies between departments. *"This often leads to problems, so we strongly recommend consolidation. And Smart ID PKI is of course very well-suited for this scenario too,"* says Furuhed.





Benefits with Smart ID PKI

There is a range of benefits migrating to Smart ID PKI – it enables you to:

- Establish uniform policies, including separation of duties.
- Benefit from simplified processes.
- Comply with signature legislation worldwide.
- Use a certified solution, since Smart ID PKI is recertified for Evaluation Assurance Level 4+ according to the international standard Common Criteria for Information Technology Security Evaluation (CC).
- Issue certificates for multiple Windows domains from a single CA system.
- Use an integrated online certificate status protocol (OCSP) responder component.
- Deploy your CA on either Windows or Linux server.
- Support all important certificate enrolment protocols, including SCEP, CMC, CMP, ACME, REST and EST.

8 easy steps to replace

To replace your existing CA, follow this smooth, step-by-step process:

1. Create customer CA and certificate profiles with Smart ID.
2. Install Smart ID agent within the customer environment.
3. Establish a TLS connection between Smart ID agent and Active Directory.
4. Publish CA certificates to Active Directory and applications, to enable new certificate hierarchy to be trusted.
5. Create local administrators.
6. Issue certificates from new CA to users, things, and IT and IoT devices to replace certificates from old CA.
7. Stop operation of the old CA
8. Relax, since you now have a time-tested and future-proof solution.

nexus
INGROUPE

Function	Nexus Smart ID PKI	Microsoft ADCS
Certifications	CommonCriteria EAL 4+	
	ISO 27001	
	TISAX	
Enrollment Protocols	ACME	
	REST	
	CMP	
	SCEP & SCEP-NDES	SCEP-NDES
	Intune	
	WS	WS
	EST	
	EST-coaps	
	WinEP	WCCE
	AST	
Monitoring	PING	
Certificate formats	X509	X509
	CVC	
	V2X	
Multitenants / Multi-CA	YES	
AD Forest support	YES	Limited
Supported Usecase	Employee	Employee
Examples	Citizens	Citizen
	LTE & 5G	
	ePassport	
	Workplace	
	IOT	
	V2X	
Policy enforcement	CA Policy through Admin Workbench	Through AD group policies
Securing CA Keys	Most common HSMs	Via CSP/KSP
High performance and scalability	YES	
Signed log-files	YES	
External OCSP	YES	YES
OCSP respons for different CAs	Based on CRLs and CIL	Based on CRLs
OCSP support for RFC 6960	YES	
OCSP statistics for billing	YES	
Separate Key generation system	YES	
External Registration Authority	YES	
Certificate Transperancy	YES	
Automized Deployment	YES	
Microsoft Auto-enrollment	YES	YES
Protection against weak keys	YES	

UNLEASH THE POWER OF PKI!

UNLEASH

Do you want to know more? **Click here!**