1 About Us

Idently Systems Limited ("Idently") provides Digital Identity and PKI solutions for enterprises, professionals and individuals needing to conduct secure e-commerce, e-communication, online content delivery, and online interactions. We are on a mission to provide secure Trusted Digital Identities for Africa's digital economy.

Idently is licenced by the Communication Authority of Kenya as an Electronic Certification Service Provider (E-CSP) to issue digital certificates and support digital signatures in Kenya.

Idently is also a GlobalSign Certified Regional Partner. GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

We offer the following certificates:

- SSL/TLS Certificates
- Document Signing Certificates
- Code Signing Certificates
- Personal/Department Certificates

We offer the following solutions:

- Managed PKI
- Secure Email (S/MIME)
- Authentication and Access Control
- Digital Signing
- Certificate Lifecycle Management, Discovery and Provisioning

2 What We Do

2.1 Certificates

2.1.1 SSL/TLS Certificates

SSL/TLS certificates encrypt information, verify identity, and strengthen consumer trust. We offer both organization validated (OV) and extended validation (EV) certificates, including the addition of subject alternative names (SANs) and wildcards (not for EV SSL).

2.1.2 Document Signing Certificates

We offer Document Signing certificates that can be used to sign or seal digital documents like Adobe PDF files or Microsoft Office and OpenOffice files.

2.1.3 Code Signing Certificates

Code Signing removes the “Unknown Publisher” security warning and identifies the publisher of a piece of software or an application.

2.1.4 Email Certificates (S/MIME)

Secure your emails by applying a digital signature, encrypting your email content, or a combination of both.

2.2 Solutions

2.2.1 Managed PKI

Managed PKI provides an overall lower total cost of ownership for PKI. The service simplifies all stages of the certificate lifecycle, including applying for and approving applications, issuing, reissuing, renewing, revoking and billing across numerous departments and locations. Managed PKI is easily deployed to any organisation, regardless of size and locality.

GlobalSign’s cloud-based Managed PKI platform centralizes all certificates across multiple business entities under one account. Automated deployment, flexible APIs for integration with enterprise systems, and comprehensive lifecycle management save time and money while keeping enterprises more secure.

For TLS (SSL) certificates GlobalSign provides a Managed SSL (MSSL) service. MSSL allows an enterprise to have one or many verified organization identity profiles from which they can instantly issue SSL certificates. MSSL takes the headache out of processing and managing an estate of certificates facilitating simple adoption. MSSL allows entities to request both organization validated (OV) and extended validation (EV) certificates from the service, including the addition of subject alternative names (SANs) and wildcards (not for EV SSL).

GlobalSign's Enterprise PKI (EPKI) similarly provides organization profile-based services for client certificates for use cases such as S/MIME, user authentication and digitally signing OOXML files (XML, MSWord and Excel and other Open Office standards). EPKI allows entities to extract certificates from a certificate licence pack across their one or many entity profiles. Both the MSSL and EPKI services are backed by APIs, Certificate Lifecycle Management and Inventory Tools making it easy to automate and track certificate deployments no matter where they originate.

GlobalSign's Managed PKI enables organizations to support BYOD (bring your own device) and secure corporate devices with mobile PKI, SCEP support, and integrations with popular MDM/EMM platforms, including AirWatch (Workspace ONE UEM) and MobileIron.

A truly one-stop PKI shop, GlobalSign makes it simple to order, renew, replace, or even revoke certificates. Users can control who issues certificates, as well as the type and to which domains/entities. Users can manage multiple departments or business entities from a single account.

2.2.2 *Secure Email (S/MIME)*

Malicious parties have become increasingly sophisticated at targeting organizations via email, including intercepting messages to view sensitive information and/or email spoofing with the intent of pushing to phishing sites or triggering malware downloads. Using S/MIME Certificates to digitally sign and encrypt emails help organizations protect themselves from these threats, by ensuring only intended recipients can access email content and also verifying the email origin to help distinguish between legitimate and malicious emails.

S/MIME, or Secure/Multipurpose Internet Mail Extensions, is the industry standard for public key encryption for MIME-based (message-based) data. S/MIME Certificates offer two key email security functions:

- **Digital Signature -** proves authorship and prevents tampering, assuring the email recipient that the email came from you, not an imposter and that the content of the email has not been altered in transit
- **Encryption -** ensures a message can only be opened by the intended recipient and keeps sensitive information from falling into the wrong hands

GlobalSign's S/MIME Certificates scale to accommodate businesses of all sizes, from individuals to small and mid-sized business to large enterprises, with certificate lifecycle management and automation technologies to simplify high volume deployments.

2.2.3 *Authentication and Access Control*

The rise of identity theft and data breaches as the result of using weak passwords strongly suggests single-factor methods of authentication (i.e. user name/ passwords) are no longer a sufficient security control. Two-factor authentication is now essential to protect organizations' sensitive data. Implement strong authentication using Digital Certificates without burdening end users with hardware tokens or applications and ensure only approved machines and devices can operate on corporate networks.

GlobalSign's strong authentication solutions utilize digital certificates for convenient and secure certificate-based and token-based two-factor authentication for the protection of enterprise networks, data, and applications, including:

2.2.4 *Digital Signing*

Despite efforts to go paperless, many organizations still find themselves relying on paper when it comes to applying signatures, which is impractical and inefficient. Digital signatures are a tried and trusted alternative to wet ink signatures and enable completely online workflows.

With GlobalSign's innovative scalable cloud-based Digital Signing Service (DSS), you can deploy digital signatures into any application with one simple REST API integration. This means all supporting cryptographic components, including signing certificates, key management, timestamping server, and OCSP or CRL service, are provided in one API call with minimal development or overhead needed and no on-premise hardware to manage. As a leader in this space, GlobalSign has designed DSS to reduce the latency and overhead that come with homegrown digital signature solutions and other, more complex integrations.

2.2.5 *Certificate Lifecycle Management, Discovery and Provisioning*

The increasingly complex requirements for discovering and managing digital certificates can be a burden for any organization. It's time-consuming, highly manual, and costly. Not only is it challenging keeping track of when certificates were issued, but companies must also be fully aware of where the certificate was installed and when it's expiring.

A Certificate Lifecycle Management (CLM), Discovery and Provisioning solution can handle all stages of lifecycle management, including the issuance, renewal and revocation of certificates. This visibility into certificate lifecycle is critical for ensuring business continuity, reducing IT operational costs, and preventing costly downtime events that impact business services.

GlobalSign's own CLM service, Auto Enrolment Gateway (AEG) is perfect for mid-size enterprises utilizing a mix of platforms and devices and looking for an automated certificate enrolment solution. The tool acts as a direct gateway between GlobalSign and the customer's Active Directory – effectively extending the reach to practically every endpoint on the corporate network. AEG makes it simple to enrol, provision and install digital certificates regardless of OS or platform.

GlobalSign's Certificate Inventory Tool (CIT) finds all SSL certificates on your networks, both internal and public-facing, regardless of the issuing CA. The resulting inventory is available in an easy-to-use portal, allowing you to run reports on usage, upcoming renewals, configurations, and CA issuance.

3 Contact Us

We would love to hear from you to discuss how we can work together. You can reach us through the following addresses:

Physical Address: *2nd Floor, Four Greenway (opposite Eden Square), Westlands Road, Westlands, Nairobi, Kenya.*

P. O. Box: *66268 00800, Nairobi, Kenya*

Telephone: *+254 734467635*

Email: *info@idently.com*