PersonalSign Digital IDs
Authenticate to online services and add trust to your documents and messages.

What is a PersonalSign Certificate?
A PersonalSign Digital Certificate is a Digital ID issued to an entity (i.e. individual or a department) that helps to prove that entity’s identity. The Digital ID binds an individual’s verified identity (typically including the name, company name and email address of the Digital ID owner) to a unique cryptographic credential. PersonalSign Certificates identify, prove and contain different levels of information.

Uses for PersonalSign Certificates
- Strong Authentication to networks, VPNs, cloud services & more.
- Secure Email-(S/MIME)- Digitally Sign & Encrypt Email
- Digitally Sign Microsoft Office Documents

Two Factor Authentication
Client Authentication is the process by which users securely access a server or remote computer by exchanging a Digital ID. Networks and web services can be configured to only allow access to particular Digital IDs. Authentication prevents unauthorized access and enhances current security. It can be used for in-browser client authentication to VPNs, smart card technology, cloud applications, and mobile devices. PersonalSign Certificates are approved Digital Certificates for various online services including the FDA ESG and NAESB Electronic Industry Registry.

Secure Email
PersonalSign Certificates use Secure/Multipurpose Internet Mail Extensions (S/MIME) technology to allow users to digitally sign and encrypt email.

Digitally signing emails protects the origin and authenticity of an email. A digital signature (different from a “message signature” or customizable salutation) adds a unique code to a message which only comes from the Digital ID of the original sender. It also confirms that the content of the email has not been altered in transit.

Encrypting email ensures message privacy. Encrypting email converts the message into (scrambled) ciphertext. Only the intended recipient (who is the owner of the corresponding private key)* can “unlock” the message and view the content in clear text. *Both the sender and the recipient must have a digital certificate to use email encryption.

Microsoft Office Document Signing
GlobalSign PersonalSign Digital IDs are trusted by Microsoft Office systems and allow you to create digital signatures. Applying a digital signature to a document proves the information originated with the signer and that the document has not been altered since the document was signed, ensuring document integrity. This allows for secure electronic document work flows, eliminates time and resources spent by replacing paper-based work flows. It also meets compliance requirements associated with electronic workflows. When applying a digital signature, you can choose to insert an image file containing a handwritten signature or other image of choice (example below).

Levels of PersonalSign Certificates
PersonalSign Certificates identify, prove and contain different levels of information:

PersonalSign 1 (Class 1):
- Proves ownership of: email address only
- Allowed usage: Secure Email & Document Signing
  - Attest to: user email address only (i.e. johnsmith@abc.com)

PersonalSign 2 (Class 2):
- Proves ownership of: identity and email address
- Allowed usage: Secure Email & Document Signing
  - Attest to: identity and email address (i.e. John Smith, john.smith@abc.com)

PersonalSign 2 Pro (Class 2):
- Proves ownership of: identity, organization details and email address
- Allowed usage: Secure Email, Document Signing and Authentication purposes.
  - Attest to: identity, organization details and email address (i.e. John Smith, ABC Company, john.smith@abc.com)

Managing Multiple Certificates- Enterprise PKI
If your organization needs to manage multiple Digital Certificates ask about GlobalSign’s Enterprise PKI (ePKI), a managed solution for GlobalSign’s Digital Certificates. The ePKI web portal provides administrators with a cost-effective and easy to use solution to simplify PKI deployments and eliminate the need to host your own Certificate Authority. With ePKI, enterprises have the necessary tools to maintain full control of their PKI requirements without the complexities and overhead cost of running an in-house CA.

For more information about GlobalSign solutions, please call (+65) 3158 0349
Visit https://wwwGlobalsign.com/en-sg/personalsign/ for more information