Permissions, Privacy and Security - Windows Apps

Permissions

The following table shows the required permissions and why our apps need it:

Commercial Name	xyzmo Signature Capture App	SIGNificant Client Signature Capture App	SIGNificant SignAnywhere App	SIGNificant SignOnPhone App
Permission				
Enterprise Authentication	not required	for Basic Authentication	not required	not required
Internet	Line-of-business: for communication with SIGNificant license server	for communication with SIGNificant server platform	for communication with SIGNificant server platform	for communication with SIGNificant server platform
Location	for GPS and WLAN location	for GPS and WLAN location	for GPS and WLAN location	not required
Private networks	Line-of-business: for communication with SIGNificant license server (within Intranet)	for communication with SIGNificant server platform (within Intranet)	for communication with SIGNificant server platform (within Intranet)	for communication with SIGNificant server platform (within Intranet)
Proximity	not required	not required	not required	used to initiate Bluetooth communication with 'xyzmo Client'
Webcam	for appending attachments, pages or picture annotations	for appending attachments, pages or picture annotations	not required	for scanning a QR code

Privacy and Security

The Apps are working with the SIGNificant server to enable the signature features. The server is typically hosted by the creator of the document or in some cases directly by Namirial.

The provided data is transferred encrypted (via HTTPS) and stored safely on the SIGNificant server. If Namirial is hosting the service, we will not share the data with others. Biometric signature data is highly encrypted via RSA and AES-256 directly on the user's device to prevent any misuse.

The following table shows which personal data is processed by our SIGNificant servers:

Namirial App	Information processed by SIGNificant server (hosted by creator of document or in some cases by Namirial)
xyzmo Signature Capture App	Standalone App (no data processed by Namirial)
SIGNificant Client Signature Capture App (SIGNificant E-Signing Client)	- RSA & AES encrypted biometric signature will be transferred and stored temporary on a SIGNificant server. The signature will just be decrypted when the biometric verification is required for the document. Encryption of the signature is done on the user's device. - Attachments & Form-Data selected or entered by the user - Geo-Location and necessary user actions for the document audit-trail
SignAnywhere App	- GUID and e-mail for licensing - RSA & AES encrypted biometric signature will be transferred and stored temporary on a SIGNificant server. The signature will just be decrypted when the biometric verification is required for the document. Encryption of the signature is done on the user's device. - Attachments & Form-Data selected or entered by the user - Geo-Location and necessary user actions for the document audit-trail
SIGNificant SignOnPhone	- GUID and e-mail for licensing - RSA & AES encrypted biometric signature will be transferred and stored temporary on a SIGNificant server. The signature will just be decrypted when the biometric verification is required for the document. Encryption of the signature is done on the users' device.

Access to the data of the document have just the creator of the document and the signer (user of apps). Responsible for transporting the document-access-link is the creator of the document (e.g. via Email). Documents typically are temporary on a SIGNificant server and will be removed after the document is finish into a protected archive. Documents at servers, hosted by Namirial, are stored temporary (time is set up by creator of the document).

All connections to the server are logged for support and metrics reasons. Therefore, the IP address and actions are stored in the log files.

Namirial doesn't share any data with others. If you have any questions about apps, privacy or security feel free to contact us.