S7 Link 73.0 — Fiche technique

Moyen de cryptologie : description technique pour la déclaration à l'ANSSI

1. Produit

Nom	S7 Link (anciennement iS7, depuis 2013)
Version	73.0 (build 24)
Type	Logiciel, application grand public pour iPhone et iPad (iOS / iPadOS 26 et ultérieurs)
Distribution	Exclusivement par l'App Store d'Apple — App Store ID 594070835, identifiant C4F.iS7
Option concernée	Achat intégré « OPC Client » (C4F.iS7.OpcClient)
Éditeur	Carlo Trotti — info@trotti.eu

2. Fonction

S7 Link lit et écrit les variables des automates programmables industriels Siemens SIMATIC S7 (S7-300, S7-400, S7-1200, S7-1500) sur le réseau local : pupitre de boutons, variables, alarmes, courbes, état et informations de la CPU. L'application ne communique qu'avec l'automate indiqué par l'utilisateur ; aucun serveur de l'éditeur n'intervient.

Deux pilotes de communication :

- **S7** (ISO-on-TCP, RFC 1006, port 102) : aucune cryptographie.
- **OPC UA** (norme internationale IEC 62541, port 4840), avec l'achat intégré « OPC Client » : la cryptographie de la norme, décrite ci-dessous.

L'application n'offre **aucune** fonction de chiffrement de fichiers, de messagerie, de VPN ou de stockage chiffré. La cryptographie ne protège que la communication avec l'automate ; l'utilisateur ne peut pas choisir les algorithmes ni les tailles de clé.

3. Bibliothèques cryptographiques

- **open62541** 1.5.10 — pile OPC UA, licence MPL 2.0 (open62541.org)
- **Mbed TLS** 3.6.7 LTS — primitives cryptographiques, licence Apache 2.0 (trustedfirmware.org)

Les deux bibliothèques sont intégrées sans modification et utilisées uniquement par le pilote OPC UA. Les autres usages de la cryptographie (HTTPS de l'App Store, trousseau iOS) sont ceux du système d'exploitation d'Apple.

4. Services de cryptologie (OPC UA Secure Conversation)

Modes de sécurité, choisis par l'utilisateur ou automatiquement selon le serveur : *None*, *Sign*, *SignAndEncrypt*.
Profils de sécurité standard OPC UA : **Basic256Sha256**, **Aes128_Sha256_RsaOaep**, **Aes256_Sha256_RsaPss**.

- **Authentification** de l'application et de l'automate par certificats X.509. Le certificat de l'automate est accepté par l'utilisateur, qui en vérifie l'empreinte SHA-256.
- **Confidentialité** des échanges (mode SignAndEncrypt) : AES-128 ou AES-256, mode CBC.
- **Intégrité** des échanges (modes Sign et SignAndEncrypt) : HMAC-SHA256.
- **Mot de passe** de l'utilisateur OPC UA : chiffré par RSA-OAEP avec le certificat de l'automate, y compris en mode None lorsque le serveur l'exige (CPU S7-1500).
- **Certificat de l'application** : X.509 auto-signé, RSA 2048 bits, SHA-256, créé sur l'appareil ; clé privée et mot de passe conservés dans le trousseau iOS (Keychain).

5. Algorithmes

Algorithme	Mode	Taille de la clé	Fonction
RSA	OAEP (SHA-1, SHA-256)	2048–4096 bits	Échange des clés de session, chiffrement du mot de passe
RSA	PKCS#1 v1.5 et PSS, SHA-256	2048–4096 bits	Signature, authentification
AES	CBC	128 et 256 bits	Confidentialité des échanges
HMAC-SHA256	NA	256 bits	Intégrité, dérivation des clés (P_SHA256)
SHA-256	NA	NA	Empreintes des certificats, signatures
CTR_DRBG (AES-256)	NA	256 bits	Génération de nombres aléatoires

Aucun algorithme propriétaire. Aucune clé n'est fournie, séquestrée ou transmise par l'éditeur.

Siemens, SIMATIC et S7 sont des marques de Siemens AG. S7 Link n'est pas affiliée à Siemens.