Технічні вимоги

Про неприпустимість використання JWT токенів як самостійного механізму в державних системах

2026

Зміст

Зміст

Анотація

ТЕХНІЧНІ ВИМОГИ

1. Нормативно-правова база

Нормативні вимоги до систем високого рівня assurance в державних та критичних інформаційних системах зобов'язують використання кваліфікованих електронних підписів на основі сертифікатів X.509 для виконання офіційних дій, підписання документів та ведення електронного документообігу.

Ключові нормативні та стандартизаційні документи:

- Вимоги до кваліфікованого електронного підпису (КЕП) на базі криптографічних алгоритмів та інфраструктури відкритих ключів (PKI) X.509.
- Політики сертифікатів (Certificate Policies — CP) державних систем високої assurance.
- NIST Special Publication 800-53 Rev. 5 та NIST SP 800-57 — рекомендації щодо управління ключами та контролю безпеки.
- IETF RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- Вимоги щодо фіксації в аудитних журналах унікальних ідентифікаторів сертифіката (серійний номер, публічний ключ, SKI, thumbprint).

Ці вимоги виключають можливість застосування JWT Token як самостійного механізму автентифікації, оскільки він не забезпечує нативного логування обов'язкових елементів X.509, потрібних для забезпечення неподільності (non-repudiation) та повної підзвітності.

2. Короткий зміст

Використання JWT (JSON Web Tokens) як основного або самостійного механізму автентифікації/авторизації в державних системах високого рівня захисту є технічно та нормативно невідповідним. Такі системи вимагають обов'язкової фіксації серійних номерів сертифікатів X.509 та ідентифікаторів публічних ключів у журналах аудиту для забезпечення неподільності, простежуваності дій та судово-медичного аудиту.

Державні фреймворки безпеки (Federal PKI, DoD, U.S. Treasury та аналогічні) базуються на інфраструктурі відкритих ключів (PKI) X.509. Журнали аудиту повинні явно містити серійний номер, публічний ключ (або SKI/thumbprint) для кожної події автентифікації чи підпису.

3. Рекомендації

У системах високого рівня assurance пріоритетним є використання автентифікації на основі сертифікатів X.509 (mTLS, PIV/CAC, смарт-карти). JWT може застосовуватися лише як допоміжний короткостроковий механізм, жорстко прив'язаний до сертифіката (cert-bound access tokens відповідно до RFC 8705).

Чистий JWT як самостійний або первинний механізм не рекомендується. Рекомендована схема:

- автентифікація через клієнтський сертифікат X.509;
- видача короткострокового cert-bound JWT;

- обов'язкове логування оригінального серійного номера сертифіката та публічного ключа на всіх етапах.

4. Практика

У реальній практиці державних систем політики сертифікатів (Certificate Policies) вимагають, щоб журнали аудиту зберігали унікальні ідентифікаційні дані сертифіката: серійний номер, публічний ключ, thumbprint або SKI. Це не опціонально для рівнів високої assurance.

JWT (RFC 7519) є stateless bearer-токеном. Навіть при асиметричному підписанні з посиланням на X.509 (x5c/x5u) стандартні бібліотеки не забезпечують обов'язкового витягнення та фіксації цих даних у формі, передбаченій CP. Це призводить до порушення вимог non-repudiation та несумісності з FIPS 140 та HSM.

5. Адвокат

Основні причини відмови від JWT як самостійного механізму заміни X.509:

1. Відсутність нативного логування X.509 serial/public key. JWT-claims (sub, iss, kid) не містять обов'язкових для CP елементів сертифіката.
2. Bearer-природа токена. Токен пред'являється без повторного криптографічного підтвердження оригінального сертифіката, що порушує NIST AU-10 та non-repudiation.
3. Криптографічні слабкості. Бібліотеки JWT вразливі до alg:none, key-confusion, header-injection. Відкликання сертифіката не автоматично анулює JWT.
4. Регуляторна невідповідність. Державні системи вимагають PKI-центричних рішень для аудиту та відповідності Certificate Policies.

6. Сутності

- JWT (JSON Web Token) — stateless bearer-токен (RFC 7519). Не забезпечує обов'язкового зв'язку з X.509 у журналах аудиту.
- X.509 Certificate — стандартний формат цифрового сертифіката PKI (RFC 5280).
- Public Key Infrastructure (PKI) — обов'язкова інфраструктура управління сертифікатами для державних систем високої assurance.
- Журнали аудиту — повинні містити серійний номер сертифіката та публічний ключ.
- Non-repudiation — криптографічно забезпечена неможливість заперечення дій, що досягається лише через X.509.

Висновок

У компонентах керування доступом, базових сервісах та інфраструктурі інформаційних систем високого рівня захисту використання JWT Token як самостійного механізму автентифікації є неприйнятним. Обов'язковим є пріоритетне застосування автентифікації на основі сертифікатів X.509 з повним логуванням серійного номера та публічного ключа. JWT може використовуватися лише як допоміжний, короткостроковий, cert-bound елемент. Це гарантує відповідність міжнародним стандартам PKI, вимогам non-repudiation та повну підзвітність дій.

Література

[1] OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks.

[2] NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management.

[3] NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.

[4] ISO/IEC/IEEE 42010:2022. Systems and software engineering — Architecture description.

[5] IETF RFC 7519. JSON Web Token (JWT).

[6] IETF RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[7] IETF RFC 8705. OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens.

[8] U.S. Department of the Treasury X.509 Certificate Policy.