DID web 부분 키 폐기 감시에서 점검 경로와 주기의 영향 분석

김건민, 김경백
전남대학교 인공지능융합학과
e-mail : geonminkim@jnu.ac.kr, kyungbaekkim@jnu.ac.kr

Effects of Monitoring Paths and Polling Intervals on Partial Key Revocation Detection in DID web

Geonmin Kim, Kyungbaek Kim
Dept. of Artificial Intelligence Convergence, Chonnam National University

요 약

DID 문서에서 일부 키만 폐기하면 유지 키를 이용한 인증 성공만으로 폐기 적용 여부를 확인하기 어렵다. 본 논문에서는 감시 경로 범위와 시간적 표본화를 분리하고, 폐기 키를 이용한 인증 요청의 실제 승인 여부와 감시 결과를 대응시키는 평가 절차를 제안한다. 두 경로 중 하나에 이전 키 집합을 일시적으로 제공하고, 두 호스트와 실제 리졸버 2종에 같은 위상 일정을 적용하여 호스트별 432시험을 수행하였다. 정상 경로만 점검하면 216/216시험을, 두 경로를 점검해도 84/216시험을 놓쳤으며, 예정 시각에 따른 예측과 관측은 구성별 7/108시험에서 달랐다. 이는 감시 경로와 실제 상태 관측 간격을 함께 평가할 필요성을 보여준다.

1. 서 론

DID 문서의 authentication 관계는 인증에 사용할 검증 방법을 명시하며 복수 키를 포함할 수 있다[1]. 일부 키만 폐기하면 유지 키의 인증 성공만으로 폐기 적용 여부를 확인하기 어렵다. 기존 연구[2-5]는 갱신·폐기 정보 제공을 다루지만, 실제 이용 경로의 일시적인 폐기 키 인증 승인도 감시 평가에 포함해야 한다. 본 논문은 폐기 키의 인증 승인 여부와 감시 결과를 대응시키고, 두 경로의 DID 문서 상태와 점검 주기를 통제하여 감시 범위와 점검 주기에 따른 탐지 누락 및 요청 비용을 분석한다.

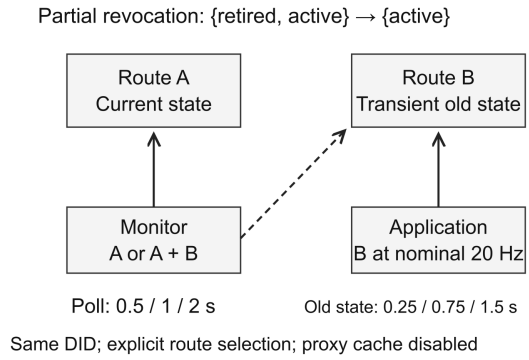
2. 관련 연구

DID-TUF는 The Update Framework로 DID 문서를 안전하게 관리·배포하며[2], CRSet은 발급자의 활동 정보 노출을 줄이며 VC 폐기 정보를 로컬에서 확인한다[3]. CRLite는 TLS 인증서 폐기 정보를 압축·배포하고[4], CTng는 정보 교환과 임계 서명으로 인증서·폐기 정보의 일관성을 다룬다[5]. 그러나 did의 한 경로에서 최신 DID 문서를 확인해도 다른 경로의 폐기 키 인증 승인 여부는 알기 어렵고, 해당 경로를 감시해도 일시적인 승인을 놓칠 수 있다.

3. 경로별 부분 키 폐기 감시 실험

3.1 경로와 반복 일정

그림 1과 같이 {폐기 대상 키, 유지 키}를 {유지 키}로 변경하였다. A는 변경된 DID 문서를, B는 서버의 키 폐기 3초 후부터 d초간 이전 DID 문서를 제공한다(d=0.25, 0.75, 1.5초). 요청 헤더로 경로를 선택하고 프록시 캐시는 비활성화하였다.



(그림 1) 경로별 오래된 상태와 감시 범위. A+B 점검은 A의 응답이 완료된 후 B를 조회한다.

회전 명령 응답 수신 시각을 t_0로 두고, 애플리케이션은 B에 $[t_0+2.2, t_0+6.5)$ 동안 0.05초 간격으로 요청을 계획하였다. 별도 리졸버로 A 또는 A+B를 점검하며, 예정 시각은 $t_0+2.2+\varphi+kT < t_0+6.5$이다($T$=0.5, 1, 2초, $k \geq 0$인 정수). A+B는 A 응답 완료 후 B를 조회하며, 서버는 20 ms 후 문서 버전을 선택한다. 요청은 응답 완료까지 기록하였다.

호스트별 두 배치(시드 719101, 719102)에서 조건별 난수 6개씩에 T를 곱해 12개 위상 φ를 생성하였다. 위상은 A와 A+B별로 생성해 두 구현·두 호스트에 동일하게 적용하고 구성별로 분석하였다. web-did-resolver 2.0.32와 did-method-web 1.0.1[6,7]의 HTTPS 경로에서 두 구현×세 d×세 T×두 감시 범위×12회로 Mac·클라우드 각각 432시험을 수행하였다. 공통 인증 규칙으로 DID·키 식별자·

수신자·nonce를 결합한 폐기 키와 유지 키의 서명 도전을 검사하였다.

3.2 누락 모형과 지표

탐지 누락은 애플리케이션에서 폐기 키의 인증 승인이 있었으나 감시에서 탐지하지 못한 시험이다. 비용은 초기 획득을 포함한 감시 요청 수이다. 순간 관측, [0,T)의 균일 위상, 노출 전후의 충분한 점검을 가정하면 이상적 누락 확률은 식 (1)과 같다.

$$P_{miss} = \max(0,\ 1 - d/T) \qquad (1)$$

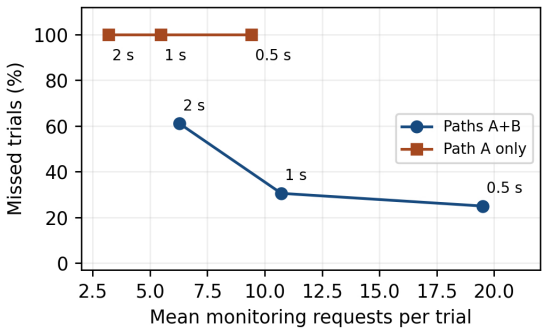
이는 고정된 12개 위상의 관측 누락률과 구분한다. 일정 기반 예측은 예정 시각의 $[t_0+3,\ t_0+3+d)$ 포함 여부로, 실제 판정은 서버가 선택한 DID 문서로 결정한다.

4. 결과 및 논의

각 호스트의 432시험 모두에서 폐기 키의 인증 승인이 관찰되었다. A는 216/216시험을, A+B도 84/216시험을 놓쳤으며, 표 1의 누락 수는 네 구성에서 동일하였다. d=0.25, T=0.5의 이상적 누락률 50%는 고정 위상의 관측 누락 9/12와 구분해야 한다. 이 조건에서는 예정·관측 누락 수가 같아도 개별 판정은 4시험에서 달랐고, 전체적으로 구성별 7/108시험이 불일치하였다. 따라서 집계값의 일치가 예측의 정확성을 보장하지 않는다. 그림 2에서 A+B의 점검 주기를 2초에서 0.5초로 줄이면 평균 요청은 6.28회에서 19.50회로 약 3.1배 증가하고, 누락은 22/36에서 9/36로 감소하였다. 이는 주기 단축의 요청 비용과 잔여 누락을 함께 고려해야 함을 보여준다.

(표 1) 이상적 확률과 실제 위상 예측 및 관측

d/T (초)	식(1) %	예정 누락	관측 누락
0.25/0.5	50	**9/12**	**9/12**
0.25/1	75	**9/12**	**10/12**
0.25/2	87.5	12/12	12/12
0.75/0.5	0	0/12	0/12
0.75/1	25	1/12	1/12
0.75/2	62.5	8/12	8/12
1.5/0.5	0	0/12	0/12
1.5/1	0	0/12	0/12
1.5/2	25	**4/12**	**2/12**



(그림 2) 주기별 요청 비용과 누락률. 구성별 세 지속시간의 각 12실험을 동일 가중했다. 네 구성의 값이 같아 공통 계열로 표시했다.

5. 결론

본 논문에서는 did:web 부분 키 폐기에서 폐기 키의 인증 승인 여부와 감시 결과를 대응시키는 평가 절차를 제안하고, 감시 경로와 점검 주기에 따른 탐지 누락 및 요청 비용을 분석하였다. 정상 경로만 점검하면 모든 노출 시험을 놓쳤으며, 실제 이용 경로를 포함해도 누락이 남았다. 따라서 감시 경로를 확보하고, 요청 비용과 허용 누락을 고려하여 점검 주기와 실제 상태 관측 간격을 함께 평가해야 한다.

Acknowledgement

본 결과물은 농림축산식품부의 재원으로 농림식품기술기획평가원의 농식품과학기술융합형연구인력양성사업의 지원을 받아 연구되었음(RS-2024-00397026)(34%). 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임(IITP-2026-RS-2022-00156287)(33%). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 인공지능융합혁신인재양성사업 연구 결과로 수행되었음(IITP-2026-RS-2023-00256629)(33%)

참 고 문 헌

[1] W3C, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, July 19, 2022. https://www.w3.org/TR/2022/REC-did-core-20220719/ (accessed Oct. 26, 2026).

[2] B. A. Alzahrani, “DID-TUF: Secure decentralized identifier management using trustless registries,” Computers & Security, vol. 162, Art. 104780, 2026.

[3] F. Hoops, J. Gebele, and F. Matthes, “CRSet: Private Non-Interactive Verifiable Credential Revocation,” arXiv:2501.17089v3, preprint, 2025.

[4] J. Larisch et al., “CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers,” IEEE Symposium on Security and Privacy, pp. 539-556, 2017.

[5] J. Kong, D. James, H. Leibowitz, E. Syta, and A. Herzberg, “CTng: Secure Certificate and Revocation Transparency,” NDSS Symposium, 2026.

[6] Decentralized Identity Foundation, “web-did-resolver,” v2.0.32, GitHub repository. https://github.com/decentralized-identity/web-did-resolver (accessed Oct. 26, 2026).

[7] Digital Bazaar, “did-method-web,” v1.0.1, GitHub repository. https://github.com/digitalbazaar/did-method-web (accessed Oct. 26, 2026).