

鍵隔離型署名

- Key Insulated Signature -



氏名
Name

佐々木 康
Ren Sasaki

坂本 恭一
Kyoichi Sakamoto

青野 光
Hikaru Aono

近

年、インターネットの普及と共に、カード番号や個人情報の流出による「フィッシング詐欺」や「なりすまし」等の被害が深刻化している。これらを防ぐために「電子署名」と呼ばれる技術がある。我々はペアリング暗号によって可能になった技術『鍵隔離型署名』用い、電子署名の作成と検証をするためのアプリケーション - The Kis - を作成した。

電子署名

Digital Signature

電子署名とは、契約書などにサインや印鑑を押したりすることを電子的に行う仕組み。ネット上でのやり取りなど、顔の見えない相手にデータが本人のものであると証明することができる。



Key Update

鍵更新

鍵更新とは、電子署名に使用する署名鍵（印鑑）を定期的に更新していく技術である。最新のものでないと署名ができないため盗難に強く、なりすまし防止につながる。



Key Insulated Signature

THE KIS

The Kis は、電子署名に鍵更新技術を応用した『鍵隔離型署名アプリケーション』である。定期的に更新される署名鍵（印鑑）を用いた、より安全性の高い署名、および検証を行うことができる。

署名鍵（印鑑）が盗難にあった場合



通常の電子署名



なりすまし詐欺を防げない



The Kis なら！



なりすましを見破る！



- 盗難された鍵を隔離（使用不可に）する
- 過去と未来の署名の安全性が保たれる