「学認・UPKI証明書・eduroam最新動向」に頂いた質問と回答

講演名	質問	回答
UPKI電子証明書 発行サービスについて	3月にGoogleより、2024年末を目安としてサーバ証明書の期限を「90日間」へ短縮する方針が示されました。世界のブラウザシェア3分の2を占めるGoogleの方針が大幅に変更されるとは思えないため、実施時期や期限が多少変わることはあってもこの方向は変わらないように思います。現状の1年期限でも既に手間が煩雑となっておりますが、これが90日となるともはや手動での管理は事実上不可能といえるレベルとなってしまいます。このままではLets Encrypt等への移行を検討せねばなりませんので、ACMEへの対応をより迅速に進めて頂きたいと考えております。	ACMEへの対応は2024年度に実施計画を具体化していく予定です。 GoogleのChrome Root Program Policyにて正式変更がありましたら、その場合は、期日に間に合うように導入を進めます。 本件、対応が遅くなり申し訳ありません。別件の、実施しないとすみやかに国際規準に違反するような内容や、事業継続に大きな影響を与える作業を優先して対応しているため、ACMEについては、具体化が遅延しております。更新作業のご負担が大きくなっていること承知しました。以前からご要望を多くいただいておりますので、優先度を上げて対応を進めます。進捗状況について、随時ご案内するようにいたします。
	グローバルサインでは、OV証明書のACME対応を行っているようですので、恐らく不可能ではないようには思います。 ACME対応の際には「Certbot」およびApache環境における「mod_md」での動作を確認して頂きたいです。可能であれば「lego」など、他のACMEクライアントでの動作確認も頂けましたら尚幸いです。	ご要望いただきありがとうございます。ご要望を考慮し、ACME対応を進めます。

「学認・UPKI証明書・eduroam最新動向」に頂いた質問と回答

講演名	質問	回答
UPKI電子証明書 発行サービスについて	ECDSA証明書については現在、サーバ側の秘密鍵にP-384のみ許可されているのに対し、署名アルゴリズムとしてはSHA256・384が許可されています。サーバ側の秘密鍵にP-256を許可しても良いと思うのですが如何でしょうか。IPAの暗号鍵ガイドラインにおいても、2040年まではP-256でも十分とされており、現在のSECOM ECCルート証明書の期限が2038年1月であることから、それまでの期間はP-256を採用しても問題無いと思われます。	ご要望承りました。次期認証局の調達を検討している段階にあり、仕様に追加できるかどうか、認証局と交渉をすすめます。
	P-256については、大半の実装で使用されている「OpenSSL」において、専用にアセンブリコードが用意されているなど、特に最適化されており、静的ホスティングにおいてはDDoS耐性の強化に繋がるほか、環境負荷低減にも寄与するのではと考えております。	
	ECCルート証明書が普及するまでの間、RSAルート証明書からクロスルート証明書を利用し、対応端末を増やすことは可能でしょうか。以前、RootCA2が普及するまでの間、RootCA1からクロスルート証明書が発行され、それを利用していたようでしたので、今回もクロスルート証明書という手段を採れる可能性を考えました。なお、現在のRootCA2もあと6年で期限切れ、かつ移行完遂期間満了になりますので、いずれにせよ移行は必要かと思われます。	クロスルート証明書を発行し、対応端末を増やすことは技術的には可能ですが、暗号方式が異なることから望ましくない点や、現在クロスルート証明書を発行するためには、Chromeの承認プロセスが必要になることから、認証局では発行しない方針としています。 Security Communication RootCA2の有効期限は、2029/05/29になります。しかし、Mozilla Root Store Policyの今後の改訂によりTLSサーバー証明書においては、2027/04/15までしか利用できない可能性が高い状況となっており、後継のRootを構築し、そちらも搭載準備をしております。進捗があり次第、ご案内いたします。

「学認・UPKI証明書・eduroam最新動向」に頂いた質問と回答

講演名	質問	回答
UPKI電子証明書 発行サービスについて	S/MIME BR対応ですが、StrictにするとE-mail Protectionのみになり利用者目線で各個人がメール用・認証用と使い分けなくてはならなくなり、利便性が著しく低下すると思われます。現状なぜ MultipurposeではなくStrictで検討されている検討状況等教えていただけないでしょうか？	今後規定が厳しくなり、「Legacy」や「Multipurpose」が廃止される状況を想定し、最も厳格な「Strict」を採用しています。 メリットとしては「Strict」に対応することで、今後のBR規定変更が発生した場合、プロファイル変更回数を減らすことが可能だと考えております。
eduroam JPについて	基地局マップですが、１台１台のAPの場所を記述するのはセキュリティ的な問題を感じます。１つの建物を指定してそこに何台あるとか、建物のフロアを指定してそこに何台あるとか、サービスエリアを図で表示するとかの方法が実現できるとよいと思いますが、いかがでしょうか？？	ご意見ありがとうございます、基地局マップにおける位置（座標を指定します）は必ずしも１台の AP に対応させる必要はございません。基地局を表現する要素として <AP_no> があり、これは AP 数を意味します。これを使うことにより、ご指摘のように「１つの建物を１点で指定し、その建物にある AP 数を設定する」ことは可能です。
	eduroamビジター用アカウントを発行&利用する際、学会等イベント終了後、PCの接続設定を削除するよう求められております。この辺りの注意書きが、PDF形式で一括ダウンロードできる同意書のどこかに記載してあると便利かと思います。	回答作成中
	現在、RADIUSを用意して eduroam を利用させていただいていますが、代理認証システムを併用することは可能でしょうか？	可能です。ただし、代理認証システムは今年度末をもって停止いたしますので、認証連携IDサービスとの併用をご検討ください。
	認証連携IDサービスのアカウントはランダム文字列@realmとなっているが、(802.1X認証の)パスワードは各大学のSSOで使われているパスワードになるのか? 別のパスワードを設定することはできないのか? (eduroamを通したパスワードのブルートフォース試行はされたくない)	大学のSSOで使われているパスワードにはなりません。アカウント発行時にランダムなパスワードが設定されます。認証連携IDサービスでは利用者が発行済みの eduroam アカウントとパスワードを確認できますが、そのパスワードを変更することはできません。

「学認・UPKI証明書・eduroam最新動向」に頂いた質問と回答

講演名	質問	回答
eduroam JPについて	eduroamのビジター用に払い出すアカウントのPWが かなりセキュア（複雑）だと思います。 安心である反面、ゲストにお伝えする時に入力ミスで 逆に手間がかかるときもあります。 ビジター用だけでも、PW指定してアカウント作成可能な機能は検討いただけますでしょうか。	ご意見ありがとうございます、ビジター用に限らずすべてのアカウント種に対して eduroam のアカウントおよびパスワードをセキュアにデバイスに導入する機能を今年度開発する予定です。この機能により、利用者のアカウント名やパスワードの誤入力の問題を解決できると考えております。