Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

Article 45 eIDAS : Les coulisses

Robin Wilton - Internet Society: Regardez l'eIDAS, Article 45, un sujet qui, j'en suis sûr, est au centre des préoccupations de tout le monde. Si vous n'avez pas entendu parler de l'Article 45, ne vous inquiétez pas. Nous y arriverons très bientôt. Mais avant cela, j'ai quelques notes d'organisation. Tout d'abord, ces sessions ont un code de conduite.

Alors, assurez-vous d'en être conscient pour éviter toute mauvaise surprise. Deuxièmement, nous avons une fonction de chat et une fonction de questions-réponses. Veuillez donc soumettre vos questions via l'une de ces options. Et enfin, l'interprétation est disponible en français, espagnol et portugais. Vous devriez voir une icône en forme de globe en bas de votre écran dans Zoom pour activer la fonction d'interprétation si vous en avez besoin.

Voilà pour les consignes. Nous avons 50 minutes pour cette session, ce qui ne semblera pas suffisant, donc je ne vais pas passer du temps à vous donner de courtes biographies de tous les intervenants. Il suffit de dire qu'il vaut la peine de consulter leurs biographies en ligne, car nous avons réussi à réunir un ensemble incroyable d'experts en la matière pour cette session.

Très brièvement, nous avons Alexis Hancock du projet CertBot de l'EFF, où elle est directrice de l'ingénierie. Dennis Jackson de Mozilla, où il fait partie de l'équipe d'ingénierie cryptographique, et par cela, j'entends le chiffrement, pas la cryptomonnaie. Et Thomas Lohninger, qui est le directeur exécutif d'Epicenter. Alors, bienvenue à mon panel.

Bienvenue à vous, le public. Nous attendons avec impatience une session fascinante. Pour planter le décor à un niveau très général, l'Article 45 définit une partie d'une stratégie générale de l'Union européenne en matière d'identification numérique dans le cadre d'une initiative plus large appelée eIDAS. L'objectif principal d'eIDAS est historiquement une identité numérique pour le citoyen, et il a évolué pour inclure des fonctionnalités de type portefeuille ou, en principe, des assertions fiables.

des attributs individuels, tels que l'identité, l'âge, les qualifications professionnelles, etc. Ce dont nous allons parler aujourd'hui est une partie très spécifique de cela, l'article 55 des règlements IDS. Et, je pense, Thomas, je vais me tourner vers vous en premier, si je peux, pour étoffer cette image très sommaire que j'ai donnée avec une petite explication de ce qu'est l'article 45, si vous le pouvez, et ensuite peut-être que nous continuerons avec certaines des caractéristiques plus larges de l'eIDAS en tant que schéma.

Thomas Lohninger - epicenter.works: Très heureux de le faire. Merci, Robin. J'espère que tout le monde m'entend bien. Oui, le règlement eIDAS est en fait une loi très ancienne. Elle a été adoptée pour la première fois en 2014. Et la mission principale de cette loi européenne est d'établir une plateforme harmonisée pour l'identité numérique. Cette loi de 2014 n'a jamais vraiment abouti parce qu'il y avait des raisons pour lesquelles les États membres nationaux, les États membres de l'UE, ne voulaient pas reconnaître tous les différents systèmes d'identité numérique des autres pays. Et donc, en juin 2021, l'Union européenne a commencé à réformer ce règlement eIDAS, et il contenait essentiellement deux grands projets. L'un était le soi-disant portefeuille d'identité numérique européen, qui devrait vraiment établir un système harmonisé pour identifier les personnes physiques et morales, comme les individus et les entreprises, vis-à-vis du secteur public et privé, en ligne et hors ligne et en proximité physique, et permettre également la vérification des attributs de ces personnes, en ligne et hors ligne. Et cela est important car il est également censé être un système universel à usage général.

Cela devrait donc vraiment couvrir les permis de conduire, les euros numériques, les contrôles aux frontières, tous les différents types de société, même les visites chez le médecin. Tout se fera sur la base de ce portefeuille d'identité numérique européen. Et la deuxième partie de cette réforme était Quox, l'article 45, qui nous amène ici aujourd'hui, où cette idée de vouloir identifier tout le monde s'étend également aux sites web.

Et, comme nous l'expliquerons bientôt plus en détail, cela a établi cette idée d'authentifier les propriétaires, les personnes derrière un site web, auprès des utilisateurs qui utilisent ou visitent un site web. Et donc cette idée d'identifier la propriété d'un domaine avec un certificat que les fournisseurs de navigateurs sont également obligés d'afficher à leurs utilisateurs est en quelque sorte une vieille idée, mais une idée que l'Union européenne veut remettre sur la table, peut-être pour aborder certains des arguments que nous avons entendus lors du débat, pourquoi certains des États membres pensent que c'est une bonne idée.

Nous, en tant qu'Epicenter Works, avons travaillé sur cette réforme dès le premier jour. Je dois dire que notre principal objectif était le portefeuille, car en tant qu'ONG de protection de la vie privée, c'était quelque chose où nous voyons une attaque drastique contre l'anonymat en ligne, sur nos données d'identité vérifiées cryptographiquement par le gouvernement, se propageant à des domaines où elles ne devraient vraiment pas être, comme les grandes entreprises technologiques ou les agences de notation de crédit. Mais nous étions également préoccupés par l'article 45 et cette attaque contre l'architecture de confiance du World Wide Web. Et je pense que je vais m'arrêter là.

Robin Wilton - Internet Society: Merci. Les 5 euros que je t'ai donnés pour cette transition parfaite étaient bien dépensés. Parce que je pense que là où tu t'es arrêté, oui, il y a ces implications potentielles pour la vie privée en ayant, ce qui pourrait en pratique être une identité émise par le gouvernement central qui est utilisée comme base pour toutes ces assertions de niveau d'attributs et je pense que nous y reviendrons en temps voulu. Mais là où tu t'es arrêté, il y a cette idée d'identifier les sites web pour l'utilisateur final également. Et donc Alexis, je pense que j'aimerais te donner la parole ensuite, si je peux. L'idée d'identifier les sites web pour l'utilisateur, cela semble familier parce que nous avons eu le petit cadenas dans le navigateur pendant un certain temps, et puis nous avons eu la barre d'URL qui devient verte pour te dire que ce site web est vraiment celui que tu pensais visiter. Est-ce que nous réinventons cela ?

Alexis Hancock - EFF: Oui, c'était une répétition. Il n'y a pas d'autre façon éloquente de le dire, où nous avions des certificats de validation étendue et nous avons abordé cette idée de vérifier votre identité via TLS, une approche que nous avions déjà adoptée auparavant.

Et cela n'a pas tenu les promesses initiales de pouvoir attirer l'utilisateur final sur un site web pour qu'il se sente non seulement en sécurité, mais aussi pour qu'il sache que la personne ou l'entité derrière le site est bien celle qu'elle prétend être, en utilisant TLS et les certificats de validation étendue pour y parvenir.

Lorsque les certificats de validation étendue ont été proposés, nous étions à une autre époque. Le web n'était pas aussi chiffré. Le web était moins sécurisé et nous avions un écosystème où les certificats de validation de domaine n'étaient pas aussi automatisés

et n'étaient pas aussi étendus à l'utilisateur quotidien du web et aux systèmes d'entreprise que nous avons aujourd'hui.

Pouvoir automatiser ces choses et pouvoir automatiser la sécurité pour les services web, les services disponibles. Donc, nous avons des certificats EV. Et nous avons traversé ce cycle et vers 2018, je pense que les navigateurs ont largement décidé de déprécier l'interface utilisateur pour le cadenas vert parce qu'il n'accomplissait pas ce qu'il était censé faire.

À l'origine, c'était un effort considérable. Et je tiens à souligner que les certificats EV ne sont pas bon marché. Ils sont coûteux par rapport aux certificats de validation de domaine. Et c'est vraiment l'émission de certificats de validation de domaine qui a aidé le web à devenir plus chiffré. Bien plus que les certificats plus chers et plus contraignants comme la validation étendue.

Nous avons donc traversé ce cycle. Et quand j'ai vu cela, j'ai vu une répétition d'une solution à un problème qui n'a pas été à la hauteur des attentes qu'elle s'était fixées.

Robin Wilton - Internet Society: Intéressant. D'accord. Donc, les thèmes que je pense que nous abordons ici sont, comme vous l'avez dit, le TLS, la sécurité de la couche de transport, qui fournit la confidentialité.

pour les sessions de navigateur, à condition que vous disposiez d'un moyen sécurisé d'échange de clés entre le serveur et le navigateur, mais ce moyen sécurisé d'échange de clés implique lui-même que vous devez identifier correctement le serveur, sinon je pourrais obtenir une session sécurisée depuis mon navigateur, mais elle pourrait ne pas être avec le bon serveur web.

Donc, comme vous le dites, le TLS résout ce problème techniquement. Mais ensuite, il y a cette étape procédurale : est-ce que la clé publique du site web appartient bien à l'organisation qui dit posséder le site web ? Et je pense que c'est cette étape procédurale. Alors, Dennis, puis-je vous demander votre avis sur ce point ?

Parce que. et vous avez été impliqué à la fois dans la technologie de chiffrement des sessions entre les navigateurs et les sites web, mais je pense que vous et vos collègues avez également travaillé sur cette idée de transparence des certificats. Alors, comment détectez-vous les comportements malveillants parmi les propriétaires de certificats de sites web ?

Je suppose que la question que je veux essayer de résumer est la suivante : si vous voulez dire à quelqu'un que ce site utilise un faux certificat pour prétendre qu'il n'est pas ce qu'il est. L'utilisateur final est-il la bonne personne à informer ?

Dennis Jackson - Mozilla: Merci, Robin. Oui, je pense que c'est une question vraiment intéressante. Donc, du point de vue de l'utilisateur final dans le navigateur, en tant qu'agent utilisateur, nous devons décider si les clés que nous voyons, le certificat que nous voyons, sont dignes de confiance pour ce site web particulier.

Et je pense que, comme vous l'avez suggéré, bien que nous puissions prendre certaines décisions techniques à ce sujet, en fin de compte, l'utilisateur ne sera jamais en mesure d'être pleinement informé sur ce site web et ses pratiques et politiques particulières, et de comprendre si ce site web est la bonne source d'information d'authentification pour cette connexion particulière.

À l'époque des certificats EV, comme l'a mentionné Alexis, nous pensions que peut-être ajouter plus d'informations à ce certificat pourrait aider les utilisateurs à prendre cette décision, et comme Alexis l'a mentionné, cette approche n'a pas vraiment été couronnée de succès. Donc, ce qui s'est passé à la place, c'est que nous nous sommes orientés davantage vers un système de transparence publique.

Et maintenant, lorsque les autorités de certification émettent les certificats utilisés dans TLS, ils doivent être enregistrés publiquement auprès de plusieurs opérateurs de journaux de transparence. L'intérêt de cela est que ces journaux sont désormais accessibles au public. En particulier, le propriétaire du site web, un chercheur en sécurité ou toute autre personne peut examiner ces journaux et consulter les certificats qui ont été émis.

Et en particulier dans le cas du propriétaire du site web, il peut dire : je reconnais ce certificat et cette clé publique parce qu'ils m'appartiennent. Je les ai générés, je les ai demandés, et donc ils sont sécurisés. Mais s'ils voient quelque chose qu'ils n'ont pas demandé, quelque chose qui ne leur appartient pas, mais qui est utilisé pour approuver une connexion à leur site web, ils peuvent signaler cela comme un problème sérieux et finalement prendre des mesures pour sécuriser les connexions à leur site web.

Robin Wilton - Internet Society: Alors que cela, ce serait, c'est quelque chose que l'individu ne peut vraiment pas faire. donc oui, leur dire que c'est faux alors qu'ils n'ont pas les moyens de faire quoi que ce soit à ce sujet. Cela pourrait finir par frustrer les gens. Cela dit, je me demande combien de personnes dans l'audience ont vu un avertissement de certificat apparaître dans leur navigateur disant, Oh, le certificat de ce site web peut être invalide.

Et combien de personnes en réalité. soit se retirent ou essaient de faire quelque chose à ce sujet au lieu de simplement cliquer et dire, ah, je voulais y aller de toute façon. et je soupçonne que la grande majorité tomberait probablement dans cette dernière catégorie. Thomas, je veux revenir à vous ici parce que Dennis a mentionné les pratiques et politiques des sites web.

En d'autres termes, qu'est-ce qu'il vous faut, en plus de la technologie, pour avoir une certaine assurance que le certificat d'un site web donné appartient vraiment à cette organisation ? Et Alexis a parlé un peu plus tôt des certificats EV, qui impliquent, par exemple, qu'une personne de l'organisation fournisse une preuve d'identité beaucoup plus solide et une preuve de son rôle au sein de l'organisation pour obtenir ce certificat.

Mais, donc la question spécifique que je voulais vous poser est, et cela se rapproche vraiment beaucoup de l'Article 45 ici, quelle est la différence entre les certificats envisagés par l'Article 45, ces soi-disant QOCS, Certificats d'Authentification Web Qualifiés, quelle est la différence entre ceux-ci et les certificats TLS qu'Alexis a mentionnés, qui après tout sont la base de cette session chiffrée entre votre navigateur et le site web ?

Thomas Lohninger - epicenter.works: Merci, Robin. C'est une excellente question et en fait, c'est une question que nous avons longuement discutée au cours des trois ans et demi depuis que cette loi a été proposée. Et, vous entendriez différentes choses de la part des législateurs et aussi des prestataires de services de confiance, qui sont les entreprises qui ont à gagner économiquement de l'Article 45.

Et certains d'entre eux diraient que ce sont vraiment deux choses différentes. Les quarks sont en réalité juste un autre mot pour les certificats de validation étendue (EV) qui sont destinés à identifier le propriétaire d'un site web affiché pour les utilisateurs, et cela suit cette idée européenne que tout doit être identifié. Nous avons une forte poussée dans diverses législations sectorielles comme la loi sur les services numériques où la vérification de l'âge est une chose.

Espace européen des données de santé, vous le voyez apparaître partout ces jours-ci, l'UE semble être assez, gravée dans le marbre, que vous voulez vraiment éradiquer l'anonymat en ligne, ce que nous considérons comme un énorme problème. Et d'ailleurs, nous avons également un droit à la pseudonymie dans l'eIDAS à l'Article 5 qui tente de réduire ce risque.

Et l'article 45, bien sûr, a une double fonction. Donc certaines personnes, et nous avons pu convaincre la majorité au Parlement européen de suivre cette interprétation, que les QUOX ne sont pas des certificats TLS. Les QUOX devraient être séparés. Les QUOX devraient se limiter à l'identification et séparer le chiffrement de bout en bout via TLS du certificat QUOX serait la bonne voie à suivre.

au Conseil, donc lorsque les 27 nouveaux États membres ont dû parvenir à un accord sur cette loi, cette distinction n'était pas si claire. Et, les prestataires de services de confiance sont généralement assez proches de leur gouvernement, ce sont des organisations nationales. Il y avait une pression pour que les prestataires de services de confiance soient reconnus par tous les fournisseurs de navigateurs.

Et vous entendriez parfois des arguments comme, oui, mais c'est tellement contraignant de figurer sur la liste d'Apple ou de Google ou de n'importe quel fournisseur de navigateur et leur magasin de certificats racine. Et si le gouvernement dit que c'est sécurisé et que c'est suffisamment sécurisé pour l'État, alors cela doit aussi être suffisamment sécurisé pour ces grandes entreprises technologiques.

C'est un argument que nous avons beaucoup entendu lors des négociations. Et pour peut-être aussi revenir sur notre situation juridique. En mai de cette année, l'Union européenne a approuvé le règlement eIDAS qui est déjà en vigueur. Mais il y a ce qu'on appelle des actes d'exécution qui détaillent les obligations de la loi.

Et il y a aussi un acte d'exécution sur l'article 45, mais nous ne l'avons pas encore vu. Au total, il y a environ 28 actes d'exécution, parfois plusieurs pour une seule disposition légale, et seulement cinq ont été soumis à consultation jusqu'à présent. La consultation s'est terminée début septembre et en fait, demain aura lieu le vote sur ces cinq actes qui concernent uniquement le portefeuille.

Nous avons en fait travaillé de très près sur ce sujet et il semble qu'ils pourraient échouer. Vous pouvez lire dans les médias politiques et allemands qu'il y a une grande frénésie entre les États membres sur la question de savoir si ces cinq actes d'exécution seront même adoptés. Cela signifie que nous devrons attendre un certain temps avant d'obtenir les détails techniques sur la manière dont les quarks sont réellement mis en œuvre et, Etsy, qui est une organisation de normalisation travaillant également en partie sur la surveillance.

les normes et l'interception légale ont également leur mot à dire dans ces spécifications techniques. Donc, le dernier mot n'est certainement pas encore dit, mais c'est vraiment bien que nous puissions avoir cette discussion.

Robin Wilton - Internet Society: Je pense que vous nous avez donné un aperçu vraiment important des coulisses, car je suis sûr que ce n'est pas une coïncidence si vous avez mentionné 28 actes d'exécution différents pour cela.

Et ce nombre semble coïncider, de près, avec le nombre d'États membres de l'UE, à un ou deux près, malheureusement. Ils l'ont compris, je pense, car vous avez également dit que vous avez entendu l'argument : si c'est suffisamment sécurisé pour satisfaire le gouvernement, alors cela devrait convenir aux citoyens.

Et pourtant, à travers ces plus de 20 États membres, nous voyons des gouvernements de teintes politiques extrêmement différentes et très complexes. Donc, ce que vous dites vraiment, c'est que d'un côté, nous avons cet ensemble global de règles sur la manière dont les certificats TLS sont intégrés dans la liste de confiance des principaux navigateurs. Et d'un autre côté, nous voulons peut-être jusqu'à 27 règles nationales différentes sur la manière dont ces certificats sont intégrés dans la même liste.

Et cela me semble être le cœur absolu de ce problème. Donc, avec cela, Alexis, puis-je m'adresser à vous un instant ? Nous avons évoqué l'idée qu'il existe un ensemble de règles par lesquelles les certificats TLS sont intégrés dans les navigateurs. Et comme l'a dit Dennis, ceux-ci reposent à leur tour sur des politiques et des procédures concernant la manière dont les autorités de certification allouent et attestent ces certificats.

S'agit-il des mêmes règles pour les certificats QOX, car cela ne semble pas être le cas.

Alexis Hancock - EFF: Donc non, et je veux examiner cela sous l'angle d'un incident de sécurité avec un certificat mal émis ou émis de manière malveillante. Il y a quelques années, le gouvernement du Kazakhstan avait essentiellement inséré un certificat pour espionner le trafic de ses citoyens.

Et ils ont fait cela au niveau du navigateur, car ils étaient auparavant de confiance. Et une fois que Mozilla l'a découvert, une fois que Chrome l'a découvert, ils ont été déchus de leur confiance parce qu'ils agissaient non seulement en dehors du cadre des droits civils en général, mais aussi de manière inappropriée en tant qu'autorité de certification. Ce n'est pas quelque chose qu'une autorité de certification est censée faire.

Et une partie de cela consiste à pouvoir agir rapidement. Ainsi, une fois que les gens ont pris conscience de ce qui se passait au niveau de la surveillance, le CA et le certificat du Kazakhstan ont été supprimés et ils ont perdu leur confiance. Lorsque vous introduisez la loi dans ce processus sans consulter les parties impliquées, cela ralentit considérablement la réponse aux incidents de sécurité, car les navigateurs devraient alors passer par un processus juridique juste pour retirer un CA ou un QTSP s'ils agissaient en dehors des limites.

Parlons maintenant de ces limites, d'accord ? Donc, vous avez des programmes Rootstore. Désormais, chaque navigateur majeur en a un. Cela n'a pas toujours été le cas. J'aime toujours mentionner cela parce que dans cette conversation des trois dernières années, on aborde TLS et l'écosystème comme s'il s'agissait du même écosystème qu'il y a 10 ans, et ce n'est tout simplement pas le cas.

Nous avons maintenant des programmes de magasins racine. Nous avons des programmes de magasins racine qui communiquent entre eux. Vous avez des bases de référence, des lignes directrices. Nous avons la transparence des certificats. Nous avons des contrôles de compte plus stricts. Il y a tout un tas de choses qui se passent et qui sont plus utiles qu'auparavant. Donc, vous avez des programmes de magasins racine, leurs règles et leur processus d'audit maintenant.

Et pas seulement les magasins de racines, mais aussi, quiconque décide qu'une AC peut y entrer, mais un véritable processus permettant de surveiller, auditer, et un processus transparent pour expulser cette AC si nécessaire. Il y a donc déjà un processus en place. Le QTSP avec Quox et l'Article 45 pourrait complètement

contourner ce processus et être automatiquement approuvé dans les magasins de racines du navigateur.

Vous pouvez donc voir maintenant où se situerait le chevauchement en termes de démocratie, de transparence, et à quoi cela ressemble lorsqu'une AC, essentiellement parrainée par l'État dans ce cas, est capable de contourner ces types de règles, et non seulement de les contourner, mais aussi d'être légalement obligée d'être requise dans ces navigateurs.

Et lorsque les navigateurs estiment qu'une autorité de certification ne répond pas à leurs normes, nous devons désormais suivre un tout nouveau processus juridique pour que cette autorité soit désapprouvée en cas de mauvaise émission, de mauvaise gestion ou d'introduction malveillante.

Robin Wilton - Internet Society: Et donc, oui, et une partie de votre crainte est que ce processus juridique prenne du temps à se dérouler, et en fait, d'un point de vue de la sécurité opérationnelle, vous avez besoin que cela se passe beaucoup plus rapidement, sur une échelle de temps plus courte.

Thomas, je vais venir vers toi et ensuite Dennis, j'ai aussi une question pour toi.

Thomas Lohninger - epicenter.works: Eh bien. Merci, Alexis, d'avoir abordé ce sujet et tu as tout à fait raison. Il y a des obstacles supplémentaires créés par cela, mais je veux aussi faire une distinction importante. Lorsque vous regardez les considérants et le débat juridique, ce qui serait considéré comme une raison d'exclure un fournisseur de services de confiance du magasin de CA racine est quelque chose de plus comme DIGI Notar, donc une violation de sécurité à la CA. Mais s'il y avait un cas d'interception légale et qu'un fournisseur de services de confiance d'un pays, prenons un pays avec une faible règle de droit, comme la Hongrie, devait émettre un certificat, totalement légal à des fins d'agence de renseignement, par exemple, alors je ne suis même pas sûr de comment cela serait classé. Nous voulions avoir un langage plus fort autour de l'interception légale parce que c'est une préoccupation majeure pour nous.

Mais malheureusement, ce n'est pas quelque chose où nous voyons un langage fort dans la loi.

Robin Wilton - Internet Society: Oui, c'est, vous peignez un tableau inquiétant et j'allais revenir vers vous, Alexis, à ce sujet, juste avant de passer au point de Dennis. Vraiment, il me semble que. En incluant ces autorités de certification mandatées par le gouvernement dans la même liste comme si elles étaient équivalentes à celles qui y entrent via le processus d'autorité de certification et de navigateur, non seulement cela ouvre la porte à, comme vous avez donné l'exemple du Kazakhstan, et ils ne sont pas les seuls, je pense que Maurice a essayé la même chose, à un gouvernement prenant des mesures pour installer un certificat racine qui lui permettrait de, de, de décrypter et d'intercepter tout le trafic entrant et sortant de ce pays.

Mais il y a un autre type de préjudice aussi, n'est-ce pas ? Si des autorités de certification se trouvent dans la liste des racines de confiance du navigateur alors qu'elles ne sont manifestement pas dignes de confiance, qu'est-ce que cela fait à la fiabilité des autres autorités de certification qui, pour autant que l'utilisateur le sache, y sont entrées par le même processus ?

Alors, quel est l'impact sur des choses comme le TLS dans ce cas ?

Alexis Hancock - EFF: Je suis fermement convaincu qu'il faut créer des politiques Internet et technologiques en tenant compte des enjeux de demain plutôt que des seuls enjeux d'aujourd'hui. Tous les membres de l'UE ne fonctionnent pas de la même manière, comme l'a dit Thomas. Certains peuvent agir, peut-être pas en accord avec les mêmes principes démocratiques que les autres États membres de l'UE.

Donc, vous devez l'envisager sous cet angle, en étant capable de créer une politique technologique qui ne se limite pas aux lignes géopolitiques. Vous devez penser à ce qu'est réellement Internet. Et c'est une chose globale. C'est une adhésion citoyenne mondiale, sur Internet.

Et j'aimerais penser qu'à chaque fois que j'ai entendu des gouvernements parler de souveraineté et de créer des barrières sur Internet autour des frontières géopolitiques, je n'ai jamais vraiment bien dormi après avoir entendu de tels termes et nomenclatures concernant Internet. Parce que si, une fois que vous commencez à créer des politiques autour de cet aspect et que vous ne pensez pas à un aspect plus global des citoyens de l'Internet et à qui interagit avec lui, et que vous ne créez pas de politiques qui protègent les gens demain et pas seulement aujourd'hui.

Vous ne savez pas qui sera au pouvoir demain. Donc, vous devez élaborer une politique technologique pour ceux qui seront au pouvoir demain et créer ces garde-fous. L'article 45 aurait mis en danger cette garantie de confiance. Surtout si vous aviez différents partis agissant différemment au sein des États membres de l'UE.

Que se passerait-il pour un utilisateur si vous aviez un QTSP de Hongrie par rapport à un autre pays ? Où pourraient-ils même évaluer cela ? Et je crois que nous ne devrions pas imposer ce fardeau aux utilisateurs ordinaires pour évaluer cela. C'est à nous, en tant qu'experts, politiciens et éducateurs sur ce sujet, de nous mettre d'accord sur ce à quoi cela ressemble plutôt que de laisser aux utilisateurs le soin de comprendre à quoi ressemble cette confiance sur le web.

Robin Wilton - Internet Society: Oui. Et nous allons certainement devoir revenir sur les impacts en matière de confidentialité, de pseudonymat et de droits fondamentaux de cela. mais je veux faire intervenir Dennis à nouveau. Désolé, Dennis, tu as attendu patiemment. Donc, il y a quelques points que j'aimerais que tu abordes, si tu peux. et le premier suit assez bien ce que vient de dire Alexis.

Donc, l'une des objections que j'ai reçues, il y a quelques années, lorsque je faisais des recherches sur les facteurs de confiance et l'Internet ici, était que cette objection à la mise en œuvre de l'Article 45, s'opposer à cela était antidémocratique dans le sens où vous aviez une réglementation, qui avait été produite par le processus démocratique de l'Union européenne.

Et d'autre part, vous aviez une poignée relativement petite de spécialistes des autorités de certification qui disaient, non, c'est une mauvaise idée. Nous n'allons pas vous laisser faire cela. Est-ce vraiment une chose antidémocratique, ou y a-t-il une justification à voir?

Dennis Jackson - Mozilla: Je pense que, pour répondre à cela, nous devons vraiment examiner comment l'article 45 a vu le jour.

Et en 21, comme Thomas l'a mentionné, il y a eu un processus public autour de l'élaboration de cette loi et de l'identification de ce qu'elle pourrait devoir faire. Et le principal résultat de cela a été une suggestion, une exigence que les navigateurs reconnaissent ces certificats et les utilisent pour afficher ce type d'informations d'identité supplémentaires.

Et Mozilla, Edry et de nombreux autres groupes se sont engagés sur cette question et ont discuté des mérites des certificats EV par rapport aux certificats DV, etc. Et vers le milieu de 20, pardon, début 23, cette loi s'est dirigée vers sa finalisation. Et dans le processus de l'UE, cela signifie entrer en Trilog, une série de négociations finales à huis clos pour produire le texte final.

C'est seulement à ce moment-là que l'article 45 a commencé à se métastaser et à prendre un tout nouveau caractère. Et c'est au cours de ces négociations privées que de nouveaux textes ont été introduits pour imposer ces exigences aux fournisseurs de navigateurs, afin de reconnaître les QTSP de l'UE, les AC de l'UE, et de ne pas les supprimer à moins que les gouvernements de l'UE ne soient d'accord.

en termes de principes démocratiques, ce texte même a été introduit en privé, et a été convenu en privé, et a failli devenir loi essentiellement par un processus de lobbying privé qui n'était pas transparent pour le public, et dont les experts en cybersécurité et les universitaires n'étaient tout simplement pas au courant et ne pouvaient pas participer.

Ce qui s'est passé ensuite, en réaction à cela, c'est que ces ONG, les fabricants de navigateurs, les universitaires et experts en cybersécurité se sont réunis pour dire que c'était une erreur, que ce n'était pas quelque chose qui devait être fait, que cela n'apporterait aucune valeur aux citoyens européens, et ont essentiellement appelé le Parlement européen à s'y opposer.

Et finalement, le Parlement européen a choisi de répondre à cet appel et a décidé de pousser pour que ce texte soit amendé et modifié à la toute dernière minute, littéralement quelques jours avant sa publication, pour introduire de nouvelles garanties qui limiteraient l'impact de la loi et n'obligeraient pas les fabricants de navigateurs à faire confiance à ces AC sur la base d'un diktat gouvernemental.

Robin Wilton - Internet Society: Joe a posé une question dans la section Q et R, disant que les amendements à l'article 25, qui permettent de prendre des mesures de sécurité urgentes, permettant l'adhésion à la meilleure expérience utilisateur en matière de sécurité. Est-ce que cela atténue certains des problèmes ici ? Sinon, voudriez-vous en voir plus ? Dennis, je veux te donner l'occasion de répondre en premier, et je pense qu'Alexis, tu pourrais avoir des réflexions à ce sujet.

Aussi, Thomas, lève la main si tu veux intervenir sur ce point. Donc Dennis, continue pour

Dennis Jackson - Mozilla: une seconde. Oui, donc le résultat principal de ces changements de dernière minute a été d'introduire une nouvelle exception pour dire qu'aucune obligation de reconnaître les charlatans ne contredirait les droits des fabricants et distributeurs de navigateurs à authentifier les sites web de la manière et par les moyens de leur choix.

Et c'est fondamentalement la protection essentielle, qui protège contre les abus de tout cela. Bien que les navigateurs continuent de reconnaître les quacks et d'afficher ces informations d'identité aux utilisateurs, cela ne s'étend pas aux clés cryptographiques contenues dans ces quacks, et les fournisseurs de navigateurs peuvent toujours utiliser leurs propres procédures de sécurité pour cela.

Je pense donc que c'est une protection essentielle et puissante, mais tout comme avec le portefeuille, cela doit maintenant être mis en œuvre dans un acte d'exécution et concrétisé dans une norme technique. Et une partie de mon travail chez Mozilla a consisté à collaborer avec Etsy sur ce à quoi ces normes techniques vont ressembler.

Et un point central de cela a été de "fendre l'atome", si vous voulez. Donc, prendre les normes QAC existantes, où les informations d'identité et les informations TLS sont contenues dans le même certificat, et les diviser en deux pour que nous ayons ensuite un certificat TLS, qui est purement sous le contrôle du navigateur et utilise les pratiques transparentes existantes que nous utilisons depuis 20 ans.

Et puis le QAC lui-même, qui contiendra des informations sur le nom de domaine du site web et des informations sur l'identité légale du site web, mais ne sera pas utilisé pour établir ces connexions cryptées. Cela a été un processus très long pour convenir de ces normes, et ce n'est toujours pas terminé, et comme Thomas l'a mentionné, cela pourrait ne pas être terminé avant encore six mois, car différentes parties des

discussions techniques et juridiques se poursuivent, mais cela a largement réduit la pression, et je pense que le pire des cas a été évité.

Robin Wilton - Internet Society: Thomas, il semble que nous soyons passés par un processus étape par étape pour décrire ce que dit la réglementation, ce que cela signifie et quelles en sont les implications. Nous semblons être très loin des objectifs de type EI DAS que nous avons décrits au départ en termes de fonctions de portefeuille, d'amélioration de la confiance des utilisateurs, car bon sang, je n'ai pas une grande impression à ce sujet d'après cette discussion.

Mais pour le dire franchement, l'article 45 est-il adapté à son objectif ?

Thomas Lohninger - epicenter.works: Non, pas vraiment. Mais la question est, à quel but sert-il ? Et si le but est de vraiment créer de la confiance dans le World Wide Web, alors je pense qu'il était vicié dès le départ. Si l'objectif était de saper l'architecture de sécurité du web, alors le verdict n'est pas encore rendu, mais finalement, je veux revenir en arrière alors que nous parcourons maintenant la chronologie, ce qui s'est passé quand, et je peux confirmer que les négociations du Trilogue ont vraiment été un moment désastreux.

Ce n'est pas ma première loi de l'UE, je fais ça depuis 10 ans, c'est pourquoi j'ai des cheveux gris. Et, c'était un moment assez plein d'espoir lorsque nous avons organisé cette lettre de 400 universitaires et ONG qui a vraiment réussi à attirer l'attention du public sur cette question parce que l'IDAS est super technique. C'est une loi très technique et compliquée qui a été principalement négociée sans beaucoup de surveillance publique.

Je pense que nous étions la seule ONG à fournir constamment des analyses de chaque version de la loi, y compris les versions non publiques discutées en trilogue, afin de permettre un débat public et un examen minutieux de ce qui se passait réellement. Mais c'est avec cette grande lettre que nous avons vraiment pu effrayer les députés européens et la présidence du Conseil pour qu'ils reviennent à la table et nous accordent des concessions qui nous donnent maintenant une chance de nous battre lors de l'application.

Et nous avons pu, au moins, obtenir quelques-unes des principales dispositions relatives à la confidentialité dans le texte juridique et votre loi avance vraiment très lentement. Donc, une fois que vous avez quelque chose comme ça, cela dure généralement une décennie. Cela signifie donc l'effet réel en pratique sur les navigateurs des gens, sur les smartphones des gens, quand vous allez chez le médecin, chez le dentiste, au supermarché, ou à travers la frontière.

Donnez-nous encore deux ou trois ans et vous le verrez réellement, car les États membres devront alors offrir toute la gamme de ces nouvelles technologies et tout ce qui pourrait impacter notre vie quotidienne. L'un des arguments qui est notre

indicateur de succès, et qui est curieusement aussi le plus fort argument politique auprès des législateurs, est qu'un grand projet comme l'eIDAS est finalement jugé par la confiance que les citoyens lui accordent.

La fiabilité de l'écosystème que nous créons, sa résilience face aux acteurs malveillants ou frauduleux qui tentent d'abuser ou de saper le système. Et c'est encore quelque chose auquel nous devons être très attentifs. Nous devons y prêter une attention particulière. C'est pourquoi je suis en fait très attentif à la manière dont le vote se déroulera demain.

Et j'espère en fait que cela échoue. J'espère que nous aurons plus de temps et que la commission devra revoir certains de ces points. L'Acte d'exécution de l'eIDAS ne sera proposé, je pense, qu'autour de mai de l'année prochaine, donc il y a encore du temps. Et la question particulière posée par Joseph concerne le considérant 65.

Et oui, il y a un langage suffisamment clair, comme je l'ai mentionné plus tôt, pour gérer quelque chose comme une violation de sécurité d'un simple fournisseur de services avec des mesures de précaution par le fournisseur de navigateur. Ils doivent notifier la commission, les autorités nationales, mais ils peuvent agir. Lorsqu'il s'agit d'une interception légale, peut-être avec une ordonnance de silence, cela dépend du pays et des lois nationales, je ne suis pas sûr.

Et je ne suis pas convaincu que le considérant 65 soit réellement une protection suffisante pour empêcher ce type d'abus.

Robin Wilton - Internet Society: Oui, fantastique. L'une de mes questions préférées quand on me montre quelque chose comme ça et qu'on me dit à quel point ce serait merveilleux, c'est de dire, montrez-moi ce qui, dans ce système, empêche réellement l'abus de la fonctionnalité que vous décrivez.

et oui, je pense que c'est une question fructueuse à poser dans ce cas, mais je veux, il nous reste 10 minutes, et je veux utiliser une partie de ce temps, Alexis, avec vous, si je peux. donc là, vous aviez Thomas, qui travaille pour, une, une organisation spécialisée dans la compréhension, le commentaire et la tentative d'influencer ce type de législation de l'UE.

et c'est déjà assez difficile au sein de l'UE. Qu'en est-il lorsque vous commencez à examiner les implications transfrontalières de cela ? Comment expliquez-vous, Alexis, aux décideurs politiques en dehors des États-Unis ce qu'est un trilogue pour commencer ? Quels types de problèmes avez-vous rencontrés là-bas ?

Alexis Hancock - EFF: Oui, donc c'était ma première expérience avec l'apprentissage des principales différences entre les comités, la commission, les parlements, les trilogues.

Et puisque c'est ma première fois, les cheveux gris ne sont pas encore apparus. mais je suis sûr que dans quelques tours, ils le feront. essayer de comprendre cela dans le contexte de ce à quoi cela ressemble, non seulement aux États-Unis, mais à l'étranger, globalement, l'Internet. Et à quoi cela ressemble-t-il pour le web de confiance ? En tant que quelqu'un qui travaille.

Un peu comme dans une ligne plus neutre de pouvoir vanter les gains de la sécurité TLS automatisée, c'est là que cela a attiré mon attention, cela inhibe, cela entrave en fait la capacité d'automatiser les certificats TLS, en gros, et différentes structures, en particulier des structures qui en ont vraiment besoin, comme dans EIDIS, où vous avez des portefeuilles numériques, vous devez pouvoir agir rapidement, vous devez pouvoir rester au top de la sécurité d'une manière, comme jamais auparavant, si vous voulez vraiment mettre en œuvre une identité numérique à grande échelle pour quelqu'un, vous devez pouvoir avoir un système de confiance qui a du sens.

Et revenir à un système de confiance avec des points de vue plus archaïques n'avait pas de sens pour moi, et traduire cela en dehors des États-Unis et voir à quoi cela pourrait ressembler, pas les États-Unis, pas les États-Unis, l'UE, mais aussi en regardant cela aux États-Unis où ils examinent également l'identité numérique, de nombreuses manières différentes.

Ce n'est pas encore au niveau fédéral, mais différents États ont déjà mis en place des permis de conduire mobiles. Je dirais qu'un peu plus de 20 États ont mis en place des permis de conduire mobiles et ont implémenté des portefeuilles ou ont passé des contrats avec Apple et Google pour utiliser leur portefeuille dans leurs systèmes natifs, iOS et Android respectivement.

Ce que vous avez ici, c'est une influence possible. Les États-Unis se tournent vers le RGPD pour de nombreux progrès en matière de protection des données. Législation et politique, et j'avais peur que si cela passait tel quel, les gens le regarderaient comme un exemple dans l'UE, en disant d'accord, regardez, l'UE a accompli cela avec l'Article 45, peut-être devrions-nous adopter un langage similaire et l'appliquer.

Je ne sais même pas vraiment à quoi cela ressemblerait si quelqu'un d'un autre pays visitait un site web soutenu par QTSP et qu'il était potentiellement fraudé si ce système était abusé. Quels sont les moyens de contester cela ou d'obtenir une sorte de compensation ou de réparation après avoir été fraudé ?

Qu'est-ce que c'était ? À quoi cela ressemblerait-il pour quelqu'un ? Et il y a beaucoup de gens en dehors de l'UE qui utilisent des sites basés dans l'UE. Cela n'aurait pas été limité à cet écosystème unique de citoyens de l'UE. Donc, je ne suis pas vraiment sûr de ce à quoi cela aurait ressemblé, mais pouvoir expliquer cela et implorer mes, les, politiciens au sein de l'UE en disant que vous donnez l'exemple, vous avez donné l'exemple avec le RGPD, donc nous avons vraiment besoin que vous fassiez bien les choses dans ce sens, ou au moins être capable de garantir les gains de sécurité de base

ici, que nous avons obtenus au cours des 10 dernières années et ne pas revenir à une époque où le TLS était coûteux, contraignant, vous.

Et honnêtement, ce n'est pas aussi rigoureux qu'avant, ou qu'actuellement, en termes de soutien à l'automatisation et de capacité à automatiser la sécurité de manière logique pour tout le monde, et de permettre aux participants de l'écosystème de prendre les décisions comme ils le font maintenant, car c'est un processus transparent.

C'est un processus qui se déroule en dehors de l'UE, même si nous avons des membres de l'UE dans différents organismes de normalisation, ils prennent ces décisions ensemble. Ce n'est pas juste en vase clos. Donc, prendre cette décision en vase clos n'avait pas vraiment de sens pour moi. Et c'est ce que j'essayais d'expliquer aux audiences en dehors de l'UE pour ne pas nécessairement suivre ce chemin particulier si cela se produisait.

Robin Wilton - Internet Society: Oui, et je pense que nous pouvons voir cela par analogie avec d'autres produits et services. La dernière chose que vous voulez, c'est un navigateur qui ne fonctionne que dans l'UE. Ce n'est tout simplement pas ainsi que ces réseaux ou fabricants de navigateurs doivent développer des produits différents pour des marchés géographiques différents. Cela commence vraiment à éroder certains des avantages fondamentaux d'avoir un Internet mondial.

D'accord, il ne nous reste que quelques minutes. Je voudrais, pour ainsi dire, faire un dernier tour de table pour recueillir vos dernières réflexions. Dennis, es-tu optimiste à ce stade, d'un point de vue technique, et si la réponse est oui ou non, qu'en est-il de l'optimisme non technique ?

Dennis Jackson - Mozilla: Je pense que je me décrirais comme un optimiste, mais j'ai du mal à être optimiste quant au processus par lequel cela a été réalisé et à la manière dont ces réglementations et normes techniques sont actuellement rédigées.

Je pense, vous savez Donc il y a

Robin Wilton - Internet Society: un peu de cela qui est ouvert et transparent et dans le processus démocratique. Vous avez mentionné, par exemple, le Parlement européen qui a pris position contre cela, mais avant d'en arriver là, il y avait aussi des sessions à huis clos plus problématiques.

Dennis Jackson - Mozilla: Oui, et je pense que non seulement avant ce point, mais aussi maintenant après ce point, où la Commission rédigera finalement un acte d'exécution pour réaliser cela, basé sur une norme technique, et cette norme technique sera développée à huis clos à l'ETSI, ce qui nécessite un accord commercial étendu pour y contribuer.

Ce ne sera pas une norme sur laquelle tout le monde pourra donner son avis, ou comme à l'ITF, où vous avez cette norme plus participative, et cet acte d'exécution ne sera pas supervisé par le Parlement. Fondamentalement, ce sera au Conseil européen, aux États membres, de décider s'ils le jugent approprié.

Et cela limite les possibilités de contrôle et de surveillance de ces processus, rendant beaucoup plus difficile pour le citoyen européen moyen de s'engager de manière significative dans ce processus. Et cette Europe

Robin Wilton - Internet Society: Le Conseil, bien sûr, est composé de politiciens nationaux. Oui. Alors Thomas, peut-être peux-tu conclure pour nous avec quelques réflexions sur l'impact plus large de cela sur des choses comme l'anonymat et le pseudonymat, ainsi que d'autres droits fondamentaux et la technologie qui les soutient.

Thomas Lohninger - epicenter.works: Oui, bien sûr. Je suis d'accord avec Dennis. Je dis toujours que je suis optimiste de profession. Et d'une certaine manière, il est assez difficile de voir les actions de nos gouvernements exposées ici devant nous avec des conséquences dévastatrices. En même temps, il y a une raison d'espérer car nous pourrions obtenir des changements significatifs dans le processus, dans les négociations avec la pression publique.

tant que nous, en tant que public informé, en tant qu'experts de la société civile, nous insérons dans ces processus. Nous pouvons faire une différence. En fait, dans les actes d'exécution qui seront votés demain, un quart de nos amendements ont été pris en compte par la commission. Il y a donc une opportunité d'influencer réellement ces décisions si nous y prêtons attention.

Ce contrôle public est essentiel. Et nous sommes à un moment décisif. Alexis a mentionné comment les systèmes d'identité numérique prolifèrent déjà dans de nombreux États américains. Je fais partie d'un projet de l'ONU sur les infrastructures publiques numériques qui s'appuie sur le système ATAR indien et de nombreuses autres régions où ces systèmes émergent.

Je pense donc que c'est exactement le moment de prêter une attention particulière et d'utiliser ces expériences d'autres pays pour apprendre et peut-être ne pas répéter les mêmes erreurs. Et en ce qui concerne le processus concret d'eIDAS, il y a une obligation légale d'avoir une période de consultation de quatre semaines après les actes d'exécution de l'article 45.

Il y a donc un moyen d'avoir un enregistrement officiel de toutes les contributions à ce sujet. C'est une excellente opportunité pour une campagne. Et, en tant que personne qui ne sait pas comment le vote se déroulera demain et que le conseil est plus difficile que le parlement, nous sommes au moins en mesure de bloquer ces actes d'exécution.

Il y a donc certainement une chance et une raison d'espérer si nous faisons tous notre travail et continuons à prêter une attention particulière à ces questions très techniques. J'ai encore l'espoir que nous puissions parvenir à un bon résultat et que ces grands systèmes techniques respectent nos droits fondamentaux.

Robin Wilton - Internet Society: Magnifique. Écoutez, je pense que nous avons rempli nos 50 minutes avec une discussion absolument fascinante.

J'ai quelques remerciements à faire. J'aimerais remercier Seema Karaman et l'équipe de Mozilla pour avoir organisé cet atelier et ce panel, Thomas Loeninger, Dennis Jackson, Alexis Hancock. Comme promis, quelle fantastique sélection d'experts en la matière. Merci beaucoup d'avoir participé aujourd'hui, dans le cadre de la Journée mondiale du chiffrement.

Et merci à tous ceux qui se sont connectés pour écouter, participer et soumettre leurs questions. Merci beaucoup. J'espère vous parler la prochaine fois également.

Alexis Hancock - EFF: Merci.

Robin Wilton - Internet Society: Merci. Au revoir. Merci.