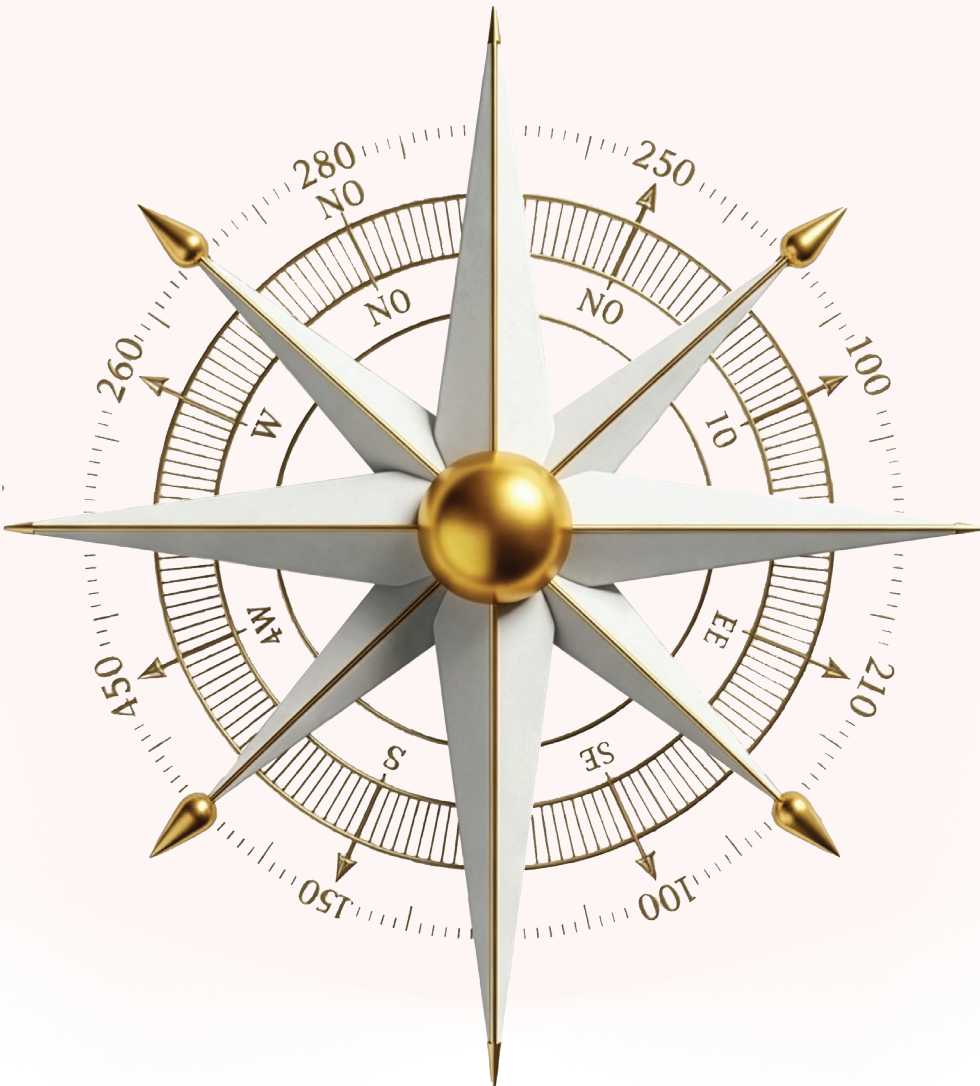




دورة البنية التحتية للمفاتيح العامة (PKI): دورة حياة الشهادات الرقمية ووحدات أمن العتاد والتشفير التطبيقي



دورة البنية التحتية للمفاتيح العامة (PKI): دورة حياة الشهادات الرقمية ووحدات أمن العتاد والتشفير التطبيقي

مقدمة:

دورة البنية التحتية للمفاتيح العامة PKI دورة تطبيقية مدتها خمسة أيام تتناول دورة حياة الشهادات الرقمية ووحدات أمن العتاد والتشفير التطبيقي، وهي موجهة لفرق معمارية الأمن والبنية التقنية والهوية والخدمات الإلكترونية، وتنتهي بإعداد تصميم PKI وسياسة لإدارة الشهادات. فالشهادات المنتهية التي توقف الخدمات الإلكترونية، ومفاتيح الإصدار ضعيفة الحماية، وفحص الإلغاء القاصر، تترك المنشأة عاجزة عن إثبات الخوادم والأجهزة والمستندات الجديرة بالثقة. ويتولى المشاركون في أعمالهم إدارة الخوادم أو أدلة المستخدمين أو ضوابط الأمن، ويتعلمون عبر مختبرات عملية على جهات إصدار الشهادات ومخازن المفاتيح وأدوات التحقق. وتقدم كور كونسبت هذه الدورة في مجال البنية التحتية للمفاتيح العامة.

أهداف الدورة:

- اختيار خوارزميات التشفير المتماثل وأزواج المفاتيح ودوال التجزئة وأنظمة التوقيع المناسبة لكل حاجة حماية في تصميم الأنظمة
- تصميم تسلسل هرمي لجهات الإصدار الجذرية والمصدرة مع أدوار جهة التسجيل وسياسة الشهادات وبيان ممارسات التصديق
- تشغيل تسجيل الشهادات وتجديدها وإلغائها مع فحص CRL وOCSP وأتمتة ACME عبر بيئات الخوادم الكبيرة
- تحديد استخدام وحدات أمن العتاد ومراسم المفاتيح وجدول تدويرها لحماية مفاتيح الإصدار والتوقيع
- توظيف الشهادات في توقيع الشيفرة والتحقق من المستندات الموقعة وهوية الأجهزة مع إعداد أدلة التدقيق لخدمات الثقة
- إعداد تصميم PKI وسياسة لإدارة الشهادات تتضمن جردا للمرونة التشفيرية والانتقال إلى ما بعد الكم لمنشأة الحالة

الفئة المستهدفة:

- فرق معمارية الأمن المسؤولة عن تحديد متطلبات التشفير والتوقيع والثقة للأنظمة والخدمات الإلكترونية الجديدة
- فرق البنية التقنية وتشغيل الخوادم المسؤولة عن تثبيت شهادات TLS وتجديدها ومعالجة أعطالها وموازنات الأحمال
- فرق تشغيل PKI وجهات إصدار الشهادات المسؤولة عن الإصدار والإلغاء والتدقيق وحماية مفاتيح جهات الإصدار
- فرق الهوية وخدمات الأدلة التي تعتمد على الشهادات في البطاقات الذكية ومصادقة الأجهزة وثقة الاتحاد
- فرق الخدمات الإلكترونية وتطوير التطبيقات المسؤولة عن توقيع الشيفرة والمستندات والمعاملات في قنوات المستخدمين والعملاء

محاورة الدورة:

اليوم 1: أسس التشفير التطبيقي وتقييم الوضع الراهن للشهادات

- خوارزميات التشفير المتماثل وأنماط التشفير الموثق لحماية البيانات
- أزواج مفاتيح RSA والمنحنيات الإهليلجية للعمليات غير المتماثلة
- دوال التجزئة ورموز مصادقة الرسائل وفحوص سلامة البيانات
- إنشاء التوقيع الرقمي والتحقق منه بالمفاتيح الخاص والعام
- مسح اكتشاف الشهادات وجرد الثقة للوضع الراهن

اليوم 2: معمارية PKI وسياسة الشهادات ونماذج الثقة

- حقول شهادات X.509 وامتداداتها وقواعد التحقق من المسار
- خيارات تصميم التسلسل الهرمي لجهات الإصدار الجذرية والسياسات والمصدرة
- إجراءات التحقق من الطلبات لدى جهة التسجيل وأدوار جهة التحقق
- هيكل سياسة الشهادات وبيان ممارسات التصديق وفق RFC 3647
- تخطيط مراسم مفتاح الجذر غير المتصل بمبدأ M من N من الأمانة

اليوم 3: عمليات دورة حياة الشهادات ووحدات أمن العتاد وإدارة المفاتيح

- طلبات تسجيل الشهادات وتوليد CSR وخطوات اعتماد الإصدار
- أتمتة تجديد شهادات TLS على نطاق واسع ببروتوكول ACME
- نشر قوائم CRL وتصميم مستجيب OCSP لفحص الإلغاء
- تقسيم وحدات أمن العتاد ونسخها الاحتياطي واعتمادها وفق FIPS 140
- حالات المفاتيح وفترات صلاحيتها وجدول تحويلها وفق SP 800-57

اليوم 4: توقيع الشيفرة وهوية الأجهزة وخدمات الثقة والمرونة التشفيرية

- شهادات توقيع الشيفرة والختم الزمني ومسارات إصدار البرمجيات
- تقارير التحقق من المستندات الموقعة وحفظ التوقيعات طويلة الأمد
- تجهيز شهادات الأجهزة وإنترنت الأشياء عند التصنيع والتهيئة
- الجاهزية لتدقيق Baseline Requirements في إصدار شهادات TLS الموثوقة علنا
- انتقالات الخوارزميات وفق SP 800-131A وجرد الانتقال إلى ما بعد الكم

اليوم 5: العمل المختبري وإعداد تصميم PKI وسياسة إدارة الشهادات

- ملخص حالة منشأة تدير خدمات إلكترونية وأجهزة وتطبيقات داخلية
- بناء مختبري لتسلسل هرمي من مستويين لجهات الإصدار وخطة وحدات أمن العتاد
- مراجعة السبب الجذري لانقطاع ناتج عن انتهاء شهادة ودليل تشغيل التجديد
- دليل الاستجابة للإلغاء وحالات اختراق مفاتيح جهات الإصدار
- استكمال تصميم PKI وسياسة إدارة الشهادات ومراجعتها من الأقران

المهارات التي ستكتسبها:

- اختيار الأدوات التشفيرية الأساسية
- معمارية التسلسل الهرمي لجهات الإصدار
- صياغة سياسة الشهادات وبيان ممارسات التصديق
- أتمتة دورة حياة الشهادات
- تصميم خدمات الإلغاء
- حفظ المفاتيح في وحدات أمن العتاد
- التحقق من توافيق الشيفرة والمستندات
- تخطيط المرونة التشفيرية

لماذا تحضر هذه الدورة:

- تسليم تصميم PKI وسياسة إدارة الشهادات إلى مجلس معمارية الأمن ورئيس البنية التقنية لاعتمادهما
- تحديد الأنظمة التي تحتاج إلى جهة إصدار داخلية أو شهادة موثوقة علناً أو مفتاح توقيع محمي بوحدة أمن العتاد
- تفادي انقطاع الخدمات بسبب الشهادات المنتهية وكلفة إعادة بناء الثقة بعد كشف مفتاح جهة إصدار غير محمي
- نقل إجراءات التسجيل والتجديد والإلغاء إلى فرق الخوادم والتطبيقات والهوية باستخدام أدلة التشغيل المختبرية

الخاتمة:

بعد عودة المشاركين يستطيع مجلس معمارية الأمن الاعتماد على تصميم PKI وسياسة إدارة الشهادات لإقرار التسلسل الهرمي لجهات الإصدار وشراء وحدات أمن العتاد وتحديد ملكية الشهادات عبر الخدمات الإلكترونية والخوادم والأجهزة. ويحصل مالكو البنية التقنية والتطبيقات على إجراء موحد للتجديد والإلغاء بدلا من المعالجات المتفرقة. وبعد أول دورة تجديد كاملة أو أول تدقيق خارجي، تراجع الوحدة حوادث انتهاء الشهادات وأوقات الاستجابة للإلغاء وجرى الخوارزميات، ثم تعدل أطوال المفاتيح ونطاق الأتمتة وخطة الانتقال.

الأسئلة الشائعة:

ما المعرفة المطلوبة قبل دورة البنية التحتية للمفاتيح العامة PKI؟

يكفي أن يمارس المشارك إدارة الخوادم أو أدلة المستخدمين أو التطبيقات أو ضوابط الأمن، وأن يفهم أساسيات الشبكات واتصالات TLS. ولا تتطلب الدورة رياضيات متقدمة، إذ تشرح مفاهيم التشفير عبر مهام مختبرية على جهات الإصدار ومخازن المفاتيح وأدوات التحقق.

كيف تختلف دورة البنية التحتية للمفاتيح العامة PKI عن دورات قانون التوقيع الإلكتروني أو إدارة الهوية؟

تبني هذه الدورة تقنية الثقة ذاتها وتشغلها: أزواج المفاتيح وجهات الإصدار ووحدات أمن العتاد وخدمات الإلغاء وأتمتة الشهادات. أما الاعتراف القانوني بالتوقيع الإلكتروني وإجراءات حوكمة الهوية فتتناولها فقط حيث تعتمد على الشهادات.

لماذا تحتاج فرق البنية التحتية للمفاتيح العامة PKI إلى المرونة التفسيرية؟

لأن الخوارزميات وأطوال المفاتيح تستبدل بمرور الوقت، وفترات صلاحية الشهادات تقصر باستمرار. وتحفظ البنية المرنة بجد لمواضع استخدام كل خوارزمية وتؤتمت إعادة الإصدار، فتتمكن المنشأة من تغيير الخوارزميات أو الانتقال نحو أنظمة ما بعد الكم دون انقطاع الخدمات.

ماذا يعود به المشارك من دورة البنية التحتية للمفاتيح العامة PKI؟

يعود كل مشارك بتصميم PKI وسياسة لإدارة الشهادات لمنشأة الحالة، يغطيان التسلسل الهرمي لجهات الإصدار وخطة وحدات أمن العتاد ومراسم المفاتيح وإجراءات دورة حياة الشهادات وتصميم الإلغاء وجرى المرونة التفسيرية، مع إمكانية تكييفها لبيئة منشأته.