Universidad de Chile
Facultad de Ciencias Físicas y Matemáticas
Departamento de Ciencias de la Computación

Perfil de Proyecto

Formulario de postulación de instituciones clientes para el Curso *Proyecto de Software CC61A*

Nombre del Proyecto:	Backend criptográfico para firmas digitales
Nombre de la Organización postulante:	NIC Labs (NIC Chile)
Nombre de la Contraparte oficial del Proyecto:	Victor Ramiro
Dirección:	Miraflores 222, Piso 14
Fono:	9407731
e-mail:	vramiro@niclabs.cl

Responsable: Agustín Villena M.
Correo Electrónico: cc61a@dcc.uchile.cl
Versión: 2009.11.23.AVM

Tabla de Contenidos

1. Información de la Organización Cliente

1.1. Breve descripción de la organización

NIC Labs es un Laboratorio de Investigación Aplicada y Transferencia Tecnológica creado por NIC Chile. Su misión es desarrollar investigación de nivel internacional generando nuevo conocimiento en el área de redes IP, buscando siempre transferir sus resultados tanto a NIC Chile, como a la comunidad nacional y regional. NIC Labs se focaliza principalmente en dos líneas de investigación y desarrollo:

- Convergencia de Tecnologías de Comunicación: hemos desarrollado varios proyectos donde mezclamos los servicios de la red telefónica con los de las redes IP.
- Redes Avanzadas, incluyendo el futuro Internet: hemos desarrollado aplicaciones para las redes inalámbricas 3G, estamos en proceso de implementar DNSSEC en NIC Chile y preparamos la migración de Chile a IP versión 6.

Como laboratorio de investigación hemos generado alianzas en proyectos con Sixbell, Entel PCS, Entel, Movistar, Claro, Telmex y VTR entre otras.

1.2. Productos fabricados o Servicios ofrecidos

NIC Labs presta servicios de investigación aplicada a problemas complejos de Ingeniería relacionados con TIC. No solo prestamos servicios de investigación al NIC Chile, sino que buscamos alianzas con empresas en sectores productivos o con el sector público. En general se nos presentan proyectos en donde investigamos diversas soluciones y prototipamos algunas de ellas para el escalamiento productivo con el cliente final.

1.3. Composición Profesional

[Incluya aquí una descripción de las personas que trabajan en su organización, cuántas son y qué perfil profesional poseen: ¿Son técnicos, operarios, periodistas, programadores, etc.?]

Nuestro laboratorio lo conforman:

- 2 Doctores en computación como Directores.
- 2 Doctores en computación como Investigadores.
- 3 Ingenieros civiles en computación como Jefes de proyecto.
- 1 Ingeniero civil en computación como Ingeniero de desarrollo.
- 2 alumnos de magíster de la U. De Chile.
- 3 memoristas de pregrado de la U. de Chile, Universidades de Santiago y Diego Portales.
- 2 estudiantes de computación como ayudantes de desarrollo.

2. Información del Problema a Resolver

Describa el proyecto desde una perspectiva de negocio, a continuación entregamos un conjunto de preguntas que debieran quedar resueltas con la descripción por usted entregada. Si le resulta más fácil puede responder la preguntas una a una, repitiendo la información en cada respuesta de ser necesario, si ya dispone de una descripción del proyecto preparada para otros efectos puede usarlas y agregar a continuación las respuestas cuyas preguntas no quedan resueltas en el documento original.

2.1. Descripción la oportunidad que desea aprovechar o el problema que desea resolver

- ¿Cuáles son los factores que lo motivan este proyecto?
- ¿Cuál es el problema o la oportunidad clave que enfrentará?
- ¿Qué pasaría si no se realizara este proyecto?

La seguridad en el sistema de nombres de dominios (DNS por su sigla en inglés) se ha ha transformado en un tema crítico. Muchos ataques se han desarrollado contra el DNS, alterando tanto la seguridad en los Servidores de Nombres como en el trafico de datos de las respuestas de DNS. Ejemplo de ello son ataques como el envenenamiento de la Cache o la suplantación de respuesta, que pueden pasar totalmente inadvertido para los usuarios normales. Las extensiones de seguridad del DNS (DNSSEC por sus siglas en inglés DNS SECurity extension) garantiza el origen de una respuesta y la autenticidad de los datos transmitidos introduciendo conceptos de criptografía de llave pública al proceso de intercambio de datos en la red. Esta solución implica una serie de desafíos en la operación y administración del servidor de DNS, en espacial para un TLD. Muchos de estos desafíos están ligados al manejo de llaves y firmas introducidos por la infraestructura de llave pública usada. En este proyecto, pretendemos desarrollar un modelo que separa las responsabilidades de operación del DNS con las de operación de la PKI, desarrollando un backend criptográfico para firmas digitales. Confiamos en que la separación de responsabilidades apoyará de manera efectiva la adopción de DNSSEC entre los principales TLDs de la región que cuentan con menos recursos que TLDs de países desarrollados, capaces de comprar y operar diversos sistemas de hardware criptográfico de alto costo. Además, proponemos un sistema en donde el manejo de llaves y firma se hace de manera distribuida. Este sistema es resistente al compromiso de un número determinado de servidores.

2.2. Descripción de la aproximación de solución

- ¿Cuáles son las funcionalidades principales que espera de la solución? ¿Cuáles son requeridos de manera más temprana? ¿Cuándo se requiere que estén listas?
- ¿Cuáles son las características claves qué se diferencia de las alternativas disponibles, por ejemplo de usar una solución manual o un software de paquete?
- ¿Cuáles son las incertidumbres o riesgos que se vislumbran en la solución propuesta? (tanto de funcionalidad para el negocio o de implementación técnica)

Un sistema como el descrito en el punto anterior requiere el desarrollo de distintos componentes que, operando de manera conjunta, sean capaces de resolver el problema de la operación de DNSSEC. En el caso de poder desarrollar dicho sistema, una primera aproximación es separar de manera efectiva la operación del DNS con la operación de la infraestructura de firma digital. Dicho esfuerzo ya se encuentra en desarrollo en nuestro laboratorio. Como paso siguiente, el desarrollo del backend criptográfico asegura la operación y uso de la infraestructura de firma digital de manera desatendida por el usuario común. Dicha funcionalidad no se encuentra disponible en ningún software disponible en la actualidad.

Como funcionalidades tempranas esperamos poder contar con un sistema capaz de resolver de manera remota comandos para la administración de llaves de firmado, certificados digitales y

realización de firmas digitales. El backend criptográfico debe considerar el cumplimiento de los siguientes requisitos no funcionales:

Seguridad: No cualquier sistema puede comunicarse con el backend criptográfico. Se debe contar con acceso restringido y con un medio seguro de comunicación.

Integridad: Se debe asegurar que la información enviada al backend criptográfico no sufra cambios en el camino. Así mismo se debe asegurar que la respuesta del backend tampoco sea alterada.

Resilencia: Se debe contar con un sistema que sea resistente a ataques, que permitan seguir operando de manera parcial o total, proveyendo el mayor uptime posible. Además se debe considerar la capacidad de recuperarse de una salida de servicio, tanto planeado como no planeado. Nótese que estos apagones pueden deberse tanto a un ataque, como a fallas naturales de hardware o desastres naturales.

Alta disponibilidad: Se debe contar un sistema que opere sin interrupciones, asegurando la mayor disponibilidad posible. Un sistema criptográfico se transforma en una pieza critica de soporte a sistemas que deben operar bajo la regla de los tres nueves de alta disponibilidad (99,9 % de uptime, corresponde a un downtime de 8,76 horas al año).

Contar con un sistema que cumpla con la totalidad de los requisitos expuestos anteriormente, conlleva una serie de dificultades, desde consideraciones de dificultad de desarrollo y su posterior operación, tanto como un alto costo de mantención a la hora de entregar un alto nivel de servicio. Nosotros proponemos el desarrollo de un sistema criptográfico distribuido para la operación del backend criptográfico. Dicho sistema toma en consideración las características presentadas anteriormente a una relación costo/seguridad mucho menor del de soluciones conocidas basadas en hardware criptográfico.

Como principal fuente de riesgo se destaca la capacidad de poner en marcha un sistema distribuido de firma digital. Si bien existen implementaciones criptográficas de prueba de concepto y referencia, nunca se ha intentado implementar un sistema de operación real basado en criptografía distribuida. Además se debe seguir con la implementación de referencia de firma digital de DNSSEC.

2.3. Descripción de los usuarios

- ¿Qué grupos o individuos se beneficiarán más de este proyecto? ¿Cuán difícil (o fácil) será para ellos adoptar la solución?
- ¿En qué forma es probable que se beneficien los usuarios iniciales? Seleccione la(s) alternativa(s) y describa
  - Ahorrar o evitar costos
  - Ahorro de trabajo o mejora de desempeño individual (por ejemplo: reducción del tiempo para completar procesos o tareas; reducción del número de pasos o simplificación de procesos o tareas).
  - Mejor desempeño organizacional (por ejemplo: mejor calidad; mayor rapidez para llegar al mercado; mayor rapidez para implementar nuevas ideas o iniciativas; menor costo y esfuerzo para tratar dentro de la organización o con los clientes, proveedores o socios).
  - Mejor acceso a información relevante y experticia (por ejemplo: creación y entrega de nueva información que haga posible una toma de decisiones mejor y más oportuna; valor agregado de información para los productos y servicios existentes; desarrollo de nuevos productos y servicios basados en información).
  - Acceso a una comunidad comprometida y leal de clientes.
  - ¿Otros?

El desarrollo de un backend criptográfico soluciona gran parte de los problemas asociados a la operación de DNSSEC. Sin embargo, un sistema como este puede ser fácilmente aplicado en otros escenarios en donde se necesite: sistemas de uso intensivo, en uptime, de firma digital, o bien una

alta resistencia a ataques, o bien ambos. A continuación detallamos algunos escenarios donde se podría aplicar un sistema como el propuesto.

Potenciales usuarios

Registry y Registrars: El origen de esta propuesta nace de la problemática encontrada en la operación continua del DNS y su dificultad de adoptar DNSSEC. Es un nicho donde el uso de una herramienta como esta puede aportar un mayor control sobre la operación de DNSSEC. Se espera una reducción de costos de operación, además de disminuir la probabilidad de tener apagones de servicio, que incrementan su probabilidad con la implantación de DNSSEC.

FF.AA.: Sistemas de inteligencia que requieran mantener y compartir información secreta se pueden beneficiar de un sistema de firmado y encriptación distribuido. En este esquema de operación se asegura una alta resilencia a ataques de denegación de servicios a nodos específicos de la red o al robo de las llaves privadas desde uno o más servidores de la red.

Bancos y Retail: Sistemas donde se quiera asegurar la autenticidad de la información de origen (estados financieros, tracking de productos inalterado, etc). El uso de un backend criptográfico de bajo costo de operación puede beneficiar e incluso proveer una ventaja competitiva en su uso. Esto se relaciona principalmente con la adopción de tecnologías como RFID y servicios basados en ONS.

3. Información sobre el Contexto del Proyecto

3.1. Plan de Implementación vislumbrado

- ¿Cuál es el equipo intra-organizacional que debe involucrarse en el proyecto? ¿Cuál es la función de cada uno?
- ¿Cuáles son las actividades claves que el equipo debe emprender y las decisiones claves que debe tomar?
- ¿Cuáles son los principales productos esperados, desde la perspectiva de negocio?
- ¿Cuál es el orden de prioridad?
- ¿Cuáles son las actividades del equipo U. de Chile? ¿Cuáles son las actividades claves del equipo interno, para transformar la entrega el producto de software en un resultado de negocio?

El desarrollo de este proyecto contempla la entrega de diversos sistemas, que en su operación conjunta, resuelven el problema de operación del servicio de DNSSEC. Como componentes de software principales podemos contar las siguientes:

1. Sistema de almacenamiento de registros DNS: Sistema que emula la mantención de los datos de zona de un servidor, tanto como un TLD como un servidor autoritativo ordinario.

2. Sistema de comunicación segura: Sistema que permite comunicación segura entre distintos sistemas, por medio de canales encriptados y transaccionales.

3. Backend criptográfico: El desarrollo del backend criptográfico se plantea de manera iterativa. Se divide en dos sistemas:
   - Proveedor de firma digital monolítico: Sistema que opera en un solo servidor físico.
   - Proveedor de firma digital distribuido: Sistema que opera en una granja de servidores. Este esquema contempla incluso distintas ubicaciones físicas de los servidores (distintas ciudades o países)

Cabe mencionar que este proyecto se encuentra en fase de desarrollo actualmente en NIC Labs. Se cuenta con dos Ingenieros a cargo del desarrollo: un jefe de proyecto y un desarrollador. **La funcionalidad propuesta para el curso de proyecto se software se concentra en el desarrollo del Backend criptográfico**. Como productos esperados, en orden de importancia, se requiere el proveedor de firma digital monolítico, y el desarrollo de una arquitectura capaz de migrar hacia un sistema de firma distribuido. Como interfaz de comunicación entre el sistema de comunicación y el backend criptográfico se encuentra un interprete de comandos XML, que recibe y valida un comando XML, lo procesa y transforma en una acción dentro del proveedor monolítico o distribuido. En segunda instancia, el desarrollo del sistema distribuido es requerido como prioridad. Finalmente el desarrollo del sistema de comunicación segura, en base a experimentos que se han desarrollado en NIC Labs.

Como actividades clave, consideramos el apoyo y validación de los modelos criptográficos teóricos y su implementación correcta en el modelo distribuido. Además de implementar de manera correcta las extensiones de los proveedores criptográficos de Java. Para una validación de correctitud, se deberá seguir un estricto proceso de testing.

3.2. Contexto de software del proyecto

[Presente cual es la plataforma sobre la cual deberá construirse el software.
Indicar si corresponde, con qué sistemas interactuará el software, describiendo sus roles y funcionalidades principales.
En el caso de que se esté desarrollando una mejora o un complemento sobre un sistema existente, debe realizarse una descripción del propósito, funcionalidades y herramientas tecnológicas sobre las que está construido el software]

La plataforma de software actual son sistemas escritos pensado en funcionar sobre plataforma Unix/Linux. En particular se cuenta con sistemas desarrollados en Java usando bases de datos MySQL. El uso de Java se basa en la interoperabilidad con software ya desarrollado en el NIC para temas de factura electrónica, además de aprovechar y explotar el desarrollo de software basado en la API estándar de Java Security.

3.3. Plataforma Tecnológica del proyecto

[Describa aquí qué recursos tecnológicos pondrá su organización para el proyecto, en cuanto a hardware y software. Sea lo más explícito posible sobre las marcas y modelos de equipos y sobre los nombres y versiones de software que posee: computadores, impresoras, redes, enlaces a Internet (tipo y ancho de banda), intranets, extranets, etc.]

Se cuenta con los servidores necesarios para el desarrollo y pruebas de operación del sistema. Además se cuenta con enlaces nacionales e internacionales de alta calidad para posibles pruebas de distribución del sistema. Se cuenta con estaciones de trabajo Dell Optiplex 755 para el desarrollo.

3.4. Inserción del proyecto en el organigrama de la organización cliente

[Debe indicarse con qué estamento y cargos se relacionarán los desarrolladores del proyecto para poder cumplir su labor. Incluya aquí, si corresponde, un organigrama de su organización, el cuál sólo se solicita para obtener más información acerca del contexto de su organización, y cómo afectará, por tanto, la introducción de un software en ella.]

Además responda

- ¿Tienen usted y el equipo gerencial el apoyo requerido para asegurar el éxito?
- ¿Quiénes son los principales apoyos para este negocio?
- ¿Por qué lo están apoyando?
- ¿Qué tipo de apoyo suministran?
- ¿Cómo venderá el proyecto a los interesados internos y externos?
- ¿Qué oposición puede interferir y cómo piensa usted superarla?

Como laboratorio de Investigación, el éxito o fracaso de nuestros proyectos se ve amenazado por las expectativas tempranas del NIC. Operamos libremente desarrollando propuestas de futuro que pueden entrar en operación en los sistemas del NIC en un plazo no definido. Por lo mismo, el desarrollo de prototipos funcionales es la mejor forma de :

- Crear pruebas de concepto que sean óptimas en la razón de recursos y beneficios. Por ello nos apoyamos en la creación de prototipos funcionales que pueden ser aprovados o descartados de manera temprana.
- Crear pruebas de concepto que logren captar la atención del NIC, de modo de asegurar su eventual uso o puesta en operación.

En particular, el desarrollo de DNSSEC para NIC Chile es un tema prioritario. Este proyecto puede ser una alternativa al actual esquema de operación de NIC Chile, en donde es necesario contar con gente especializada en el uso de nuevas plataformas y tecnologías relacionadas a DNSSEC. Este proyecto cuenta con el respaldo del Director de la laboratorio, Tomás Barros. Como apoyo extra se cuenta con el equipo de ingenieros del NIC Chile, quienes participan semanalmente en reuniones con NIC Labs para discutir sobre implementaciones y los posibles impactos de adopción de prototipos en sus sistemas de producción. Como fuente de oposición se cuenta que los ingenieros del NIC no esten de acuerdo con las decisiones de diseño y arquitectura propuestas por NIC Labs. Esto puede ser mitigado ofreciendo soluciones o puentes que permitan funcionar con ambas alternativas de manera sincronizada.

3.5. Información de las contrapartes

Información de la Organización Cliente

Razón Social	Universidad de Chile
RUT	60.910.000-1
Dirección física	Miraflores 222, Piso 14
Dirección web	http://www.niclabs.cl

Información del Responsable Institucional (Sponsor)

Nombre completo	Tomás Barros Arancibia			
RUT	10.582.158-1		Antigüedad en la organización (años)	2,5
Cargo en la organización	Director Ejecutivo Niclabs		Antigüedad	2,5
Formación Profesional	Ingeniero Civil en Computación			
Fono	940-7700	Correo electrónico	tbarros@niclabs.cl	
Dirección física	Miraflores 222, Piso 14			
Observaciones:				

Información de la Contraparte Oficial

Nombre completo	Victor Ramiro Cid			
RUT	15.541.075-2		Antigüedad en la organización (años)	1,5
Cargo en la organización	Ingeniero de Investigación		Antigüedad	1
Formación Profesional	Ingeniero Civil en Computación			
Fono	940-7731	Correo electrónico	vramiro@niclabs.cl	
Dirección física	Miraflores 222, Piso 14			
Observaciones:				

Información de la Contraparte Subrogante

Nombre completo	Pablo Valenzuela Sáez			
RUT	15.449.206-2		Antigüedad en la organización (años)	1
Cargo en la organización	Ingeniero de Desarrollo		Antigüedad	1
Formación Profesional	Ingeniero Civil en Informática			
Fono	940-7731	Correo electrónico	pvalenzuela@niclabs.cl	
Dirección física	Miraflores 222, Piso 14			
Observaciones:				

4. Información referencial

¿Cómo fue que supieron de esta iniciativa del DCC?
(Contestar todas las alternativas que sean aplicables)

Ya hemos postulado con anterioridad	¿Cuándo? no
Antiguos postulantes nos recomendaron el programa	¿Quienes? no
Somos ex-alumnos y hemos trabajado como desarrolladores en CC61A	¿En qué semestre? Semestre Primavera 2006
Recomendación directa del cuerpo docente	¿Quién? Agustín Villena
Otros	Explicitar
Referencias (Sólo para organizaciones que postulan por primera vez)	Indicar dos contactos de organizaciones externas con quienes Uds. hayan realizado proyectos anteriormente. Idealmente contactos que sean del DCC. Contacto 1: • Nombre completo: Claudio Cerda • Organización: Entel PCS • Cargo: Subgerente Ingeniería desarrollo de servicios • Fono directo: +569 98289677 • Correo electrónico: cscerda@entel.cl • ¿Relacionado con el DCC?: Proyecto Marco y proyecto de software Contacto 2: • Nombre completo: Rodrigo Perez • Organización: SixBell • Cargo: Product Architect • Fono directo: +562 2001317 • Correo electrónico: rperez@sixbell.cl • ¿Relacionado con el DCC?: Consorcio CORFO via UNTEC

5. Declaración de aceptación de condiciones para el desarrollo del proyecto

Declaración de aceptación de las condiciones de postulación
como cliente del Curso "Proyecto de Software", del DCC de la Universidad de Chile, para el semestre Primavera de 2009

En Santiago, 21 de diciembre de 2009, yo, Tomás Barros en mi rol de Director del laboratorio de investigación de NIC Chile, NIC labs, declaro aceptar los términos y condiciones definidos en el documento "Llamado a postulación de instituciones clientes para Curso Proyecto de Software CC61A":

- Un aporte de $1.400.000 al Departamento de Ciencias de la Computación como aporte a los gastos operacionales derivados de la ejecución del proyecto de desarrollo,
- Disponer en las instalaciones de mi organización de 4 (cuatro) puestos de trabajo con sus respectivos computadores, estos últimos con características técnicas adecuadas para desarrollar el software.
- Asignar una contraparte oficial y otra subrogante, ambas personas empleadas por mi organización que dispondrá de un mínimo de 8 horas a la semana para trabajar junto al equipo de desarrollo.

Todo lo anterior, una vez que esta postulación haya sido aceptada por el Departamento de Ciencias de la Computación de la Universidad de Chile.

_____ _____

Tomás Barros
Director NIC Labs
10.582.158-1
Responsable Institucional

Timbre institución