

## **Ein Archiv für Notare**

*AdNovum hat ein elektronisches Archiv für die Ablage von notariellen Dokumenten entwickelt, das den Schweizer Notaren künftig als zentraler und sicherer Service über das Internet zur Verfügung steht. Ein ausgefeiltes Rollenkonzept ermöglicht die feingranulare Vergabe von Zugriffsrechten.*

Die Schweizer Notare decken ein umfangreiches Angebotsspektrum im Bereich der vorgelagerten Rechtspflege ab. So beglaubigen sie Unterschriften oder Dokumente und sind zuständig für die öffentliche Beurkundung etwa von Firmengründungsakten, Grundbuchänderungen oder Testamenten. Im Rahmen des übergeordneten Ziels eines umfassenden eGovernments, mit dem die Interaktion zwischen Bürgern, Unternehmen und Ämtern in das elektronische Zeitalter überführt werden soll, müssen auch die Notare schon bald beglaubigte Dokumente auf Verlangen in einer elektronischen Version ausfertigen, ausliefern und aufbewahren können. Dafür wurden von Bund und Kantonen bereits verschiedene gesetzliche Rahmenbedingungen geschaffen.

Im Jahr 2004 haben verschiedene Berufsverbände und anderen Interessengruppen die Stiftung Schweizerisches Notariat gegründet. Sie bezweckt unter anderem die Schaffung von technischen Hilfsmitteln, mit denen die Vision vom elektronischen Notariat verwirklicht werden soll. Dabei geht es beispielsweise um ein zentrales Notaren-Register und ein elektronisches Archiv (eArchive) für die Aufbewahrung von notariellen Dokumenten. Dank diesen beiden koordinierten Initiativen muss in der hochgradig fragmentierten und auf kantonaler Gesetzgebung beruhenden Notariatslandschaft nicht jeder Kanton oder Notar eine eigene Lösungen für die elektronische Dokumentenverwaltung entwickeln.

### **Zentrales Notaren-Register**

Das Projekt zur Entwicklung eines zentralen, öffentlich zugänglichen Notaren-Registers wurde bereits vor einigen Jahren ins Leben gerufen. Künftig werden darin alle ermächtigten Notare der Schweiz eingetragen sein. Für jeden Notar wird darin neben persönlichen Daten auch ein vertrauenswürdige, elektronisches Zertifikat abgelegt, das eine eindeutige Identifizierung erlaubt. Der Empfänger eines notariell beglaubigten elektronischen Dokuments wird so zweifelsfrei überprüfen können, ob es sich beim Aussteller tatsächlich um eine eingetragene und ermächtigte Urkundsperson handelt.

In einem zweiten Schritt hat die Stiftung Schweizerisches Notariat die Entwicklung eines eArchive für die Schweizer Notare in Auftrag gegeben. Dem Notaren-Register kommt in diesem Zusammenhang die Aufgabe zu, anhand der dort zentral hinterlegten Informationen und Zertifikate den Zugriff auf das Archiv sowie als Identitätsprovider die individuellen Berechtigungen der Notare zu verwalten. Mit der Realisierung des eArchive und der Integration des Registers als Service wurde AdNovum beauftragt. Ausschlaggebend für diese Wahl war die hohe Kompetenz des Unternehmens in den Bereichen High-End Security und Software Engineering.

Das ambitionöse Ziel des Anfang August 2009 gestarteten Projektes war es, bis zum Stichtag per Ende Januar 2010 über einen funktionsfähigen Prototypen für das eArchive als über das Internet benutzbaren Service zu verfügen. Dieser sollte anschliessend durch rund 100 Notare aus dem Kanton Waadt einem Praxistest unterzogen werden. Der eigentlichen Entwicklungs- und Integrationsarbeit hat AdNovum eine rund zweimonatige, intensive Analyse- und Beratungsphase vorangestellt. Dabei wurde ein tragfähiges Konzept entwickelt, mit dem sich das Notaren-Register unter Berücksichtigung aller Anforderungen zu einer integrierten, sicheren Gesamtlösung für das elektronische Archivieren erweitern lässt. „Die Analyse und Beratung durch AdNovum hat uns ein lösungsorientiertes und effektives Vorgehen ermöglicht“, führt Michael Schleipen, CEO der Auftraggeberfirma SDMS aus.

## Spezialfall Schriftgutverwaltung

Die grundsätzliche Aufgabe des eArchive besteht darin, in elektronischer Form vorhandene notarielle Dokumente sicher zu verwalten und langfristig zu archivieren. Gemäss den typischen Anforderungen an ein Document Management System (DMS) muss die Lösung den ganzen Lebenszyklus der Dokumente von der Entstehung bis zur Langzeitarchivierung kontrollieren und somit Basis-Funktionalitäten wie Checkin/Checkout, ein Versionsmanagement, Suchen, Navigieren und Visualisierung abdecken.

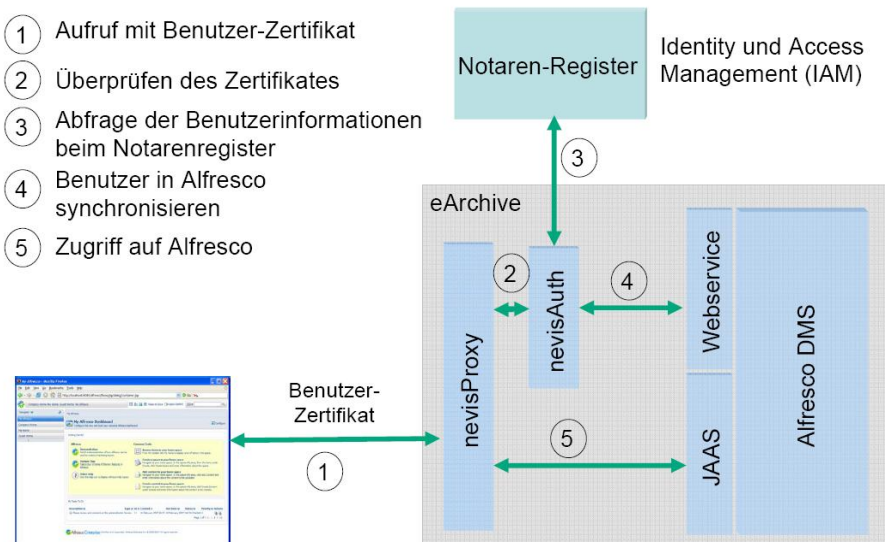
Weil es sich bei den im eArchive abzulegenden Dokumenten meistens um eingescannte notariell beglaubigte Dokumente handelt, kommen allerdings noch weitere Kriterien dazu. Für die so genannte Schriftgutverwaltung (Records Management) müssen auch Echtheit, Integrität und Benutzbarkeit gewährleistet sein, ebenso wichtig ist eine grösstmögliche Sicherheit (s. Kasten). Diverse Spezifikationen wie MoReq2 (Model Requirements Specification for the Management of Electronic Records) oder DoD 5015.02 (Electronic Records Management Software Applications Design Criteria Standard) stellen sicher, dass die in einem entsprechenden IT-System abgelegten Dokumente den Anforderungen an Schriftgüter genügen.

## Open-Source-DMS als solide Basis

Weil der Zeitrahmen vom Projektstart bis zur Ablieferung eines funktionierenden Piloten eher knapp bemessen war, kam von Anfang an nur die Verwendung und Anpassung eines bestehenden DMS in Frage. Bei der Auswahl eines geeigneten Basisproduktes stand ein optimaler Kompromiss zwischen Funktionalität und Flexibilität im Vordergrund. Unter zusätzlicher Berücksichtigung der Kosten fiel die Wahl nach einer gründlichen Evaluation verschiedener Kandidaten auf das Open Source-Produkt Alfresco. Ausschlaggebend dafür war der umfassende Funktionsumfang. Der frei zugängliche Quellcode ermöglicht zudem auch langfristig ein hohes Mass an Flexibilität und Kontrolle für die Umsetzung zusätzlicher Kundenwünsche.

Das zentrale Notaren-Register dient wie eingangs beschrieben der Verwaltung von Benutzerinformationen, insbesondere dem Eintrag und der Identifikation der Notare über elektronische Zertifikate. Für die technische Anbindung des Registers als Identitätsprovider an Alfresco hat AdNovum die selber entwickelte Architektur Nevis eingesetzt. Nevis ist ein modulares Security-Framework, das sich bereits in zahlreichen Projekten für die Entwicklung von anspruchsvollen Identity- und Access-Management-Lösungen bewährt hat. Für die Anbindung des Registers kommt dabei eine Standard-Konfiguration mit den beiden Komponenten nevisProxy und nevisAuth zum Einsatz.

## Systemübersicht



((JAAS: Java Authentication & Authorization Service))

### Sichere Anbindung über Nevis

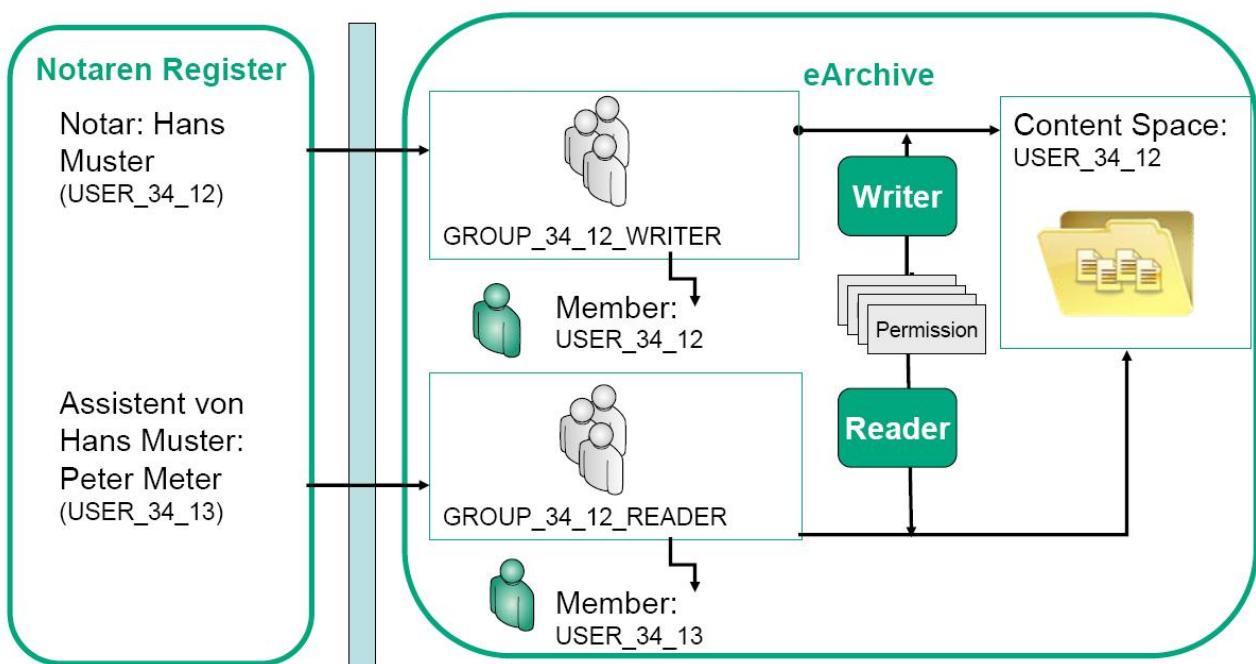
NevisProxy, ein Secure-Reverse-Proxy mit integrierter Web-Application-Firewall, agiert dabei als vorgelagerter, zentraler und einziger Einstiegspunkt für den Webverkehr in das eArchive. Der Benutzer meldet sich mit einem vom Notariatsverband vorgegebenen Zertifikat an. Wird er nicht erkannt, erfolgt die Weiterleitung an den Authentisierungs-Service nevisAuth, der für die Authentisierung des Zertifikats beim Register zuständig ist. Er fragt dort über eine verschlüsselte SSL-Verbindung an, ob der Benutzer ein eingetragener Notar ist und über welche Berechtigungen er gegebenenfalls verfügt. Das Register schickt in der Folge die groben Zugriffsberechtigungen an nevisAuth zurück.

Über eine Web-Service-Schnittstelle werden die erhaltenen Berechtigungen anschliessend direkt mit der Benutzerhaltung von Alfresco synchronisiert. Beim ersten Zugriff wird der Notar als Benutzer angelegt, gleichzeitig aber auch eine vordefinierte Ordnerstruktur als privater Ablagebereich innerhalb der DMS-Applikation erstellt. Erst nach abgeschlossener Authentisierung und Synchronisierung wird der Benutzer in die eigentliche Applikation weitergeleitet. Periodisch werden die in Alfresco enthaltenen Authentisierungs-Daten mit dem Register abgeglichen, damit abgelaufene Berechtigungen erkannt und zeitnah im Archiv reflektiert werden können.

### Ein flexibles Rollenkonzept

Eine detailliertere Betrachtung verdient an dieser Stelle das von AdNovum in der Analyse- und Beratungsphase entwickelte Rollenkonzept für Alfresco, mit dem sich auch Spezialfälle wie Nachfolge, Stellvertretung oder der notarenübergreifende Zugriff auf Dokumente abbilden lassen. Diese Flexibilität in der Vergabe von Berechtigungen stellte eine zusätzliche, zentrale Anforderung des Kunden dar. Grundsätzlich erlaubt Alfresco auf der Benutzerebene die Definition von einzelnen Benutzern oder Gruppen von Benutzern. Rollen sind Gruppierungen von bestimmten Berechtigungen. Die Rolle „Writer“ erlaubt etwa „Lesen“, „Ändern“ und „Schreiben“, die Rolle „Reader“ nur „Lesen“. Rollen lassen sich beliebig mit Benutzern oder Gruppen verknüpfen. Zusätzlich können Berechtigungen auch feingranular auf der Ebene einzelner Dateien oder Ordner vergeben werden.

### Synchronisation mit dem Register



Beim ersten Einloggen eines Notars ins eArchive werden im persönlichen Ablagebereich zwei Benutzergruppen angelegt: Eine Gruppe „Writer“ und eine Gruppe „Reader“. Die erste Gruppe ist über die Rolle „Writer“, die zweite Gruppe über die Rolle „Reader“ mit der Dateiablage verknüpft. Bei der ersten Synchronisierung wird der Notar standardmässig als Mitglied der Gruppe „Writer“ eingetragen. Er verfügt für seinen eigenen Ablagebereich also automatisch über alle in der Rolle „Writer“ enthaltenen Berechtigungen. Assistenten des Notars werden einfach als Mitglieder der Gruppe „Reader“ eingetragen und sind somit nur mit Leseberechtigungen ausgestattet. Ferienvertretungen oder Nachfolger des Notars werden für den Erhalt der vollen Berechtigungen wiederum der Gruppe „Writer“ zugeteilt. Nun lässt sich aber auch – etwa für die Mitarbeitenden des kantonalen Grundbuchamts – ein notarenübergreifender Zugriff auf Dokumente einrichten, indem diese Personen beim ersten Synchronisationsstop bei allen Notaren des Kantons in die Gruppe „Reader“ eingetragen werden. Die Trennung von Benutzern, Gruppen, Dokumenten und Ordnern von den einzelnen Rollen bringt eine hohe Flexibilität und erlaubt die Abbildung von verschiedensten, auch künftigen Szenarien.

### **Iteratives Vorgehensmodell**

Um sicherzustellen, dass die entwickelte Lösung voll und ganz den Erwartungen und Anforderungen des Kunden entsprach, wurde für die Realisierung ein hochgradig iteratives Vorgehensmodell mit kurzen Releasezyklen gewählt. Im Schnitt alle zwei Monate wurde eine installierbare Version geliefert, auf die der Kunde Feedback geben konnte. Im Rahmen dieses agilen Projektmanagements erfolgte eine schrittweise Annäherung an exakt die Lösung, die der Kunde benötigte. „Die fachliche Kompetenz kombiniert mit der äusserst kundenorientierten Vorgehensweise machte AdNovum zum idealen Partner in diesem Projekt“, beschreibt Schleipen die Zusammenarbeit.

Kasten 2700 Zeichen

### **Die Spezialitäten des eArchive für Notare**

Zusätzlich zu den Eigenschaften einer klassischen Dokumentenverwaltung verlangt die Verwaltung von Schriftgut weiterführende Funktionalitäten wie Echtheit, Integrität und Benutzerbarkeit. Ebenso wichtig ist grösstmögliche Sicherheit.

**Echtheit:** Ein Schriftgut gilt als echt, wenn Urheberschaft und Erstellungsdatum eindeutig belegt werden können. Die Identität des Urhebers muss mit dem angegebenen Autor sowie das tatsächliche mit dem angegebenen Erstellungsdatum übereinstimmen. Die Echtheit kann dabei nicht ausschliesslich durch systemtechnische Massnahmen sichergestellt werden. Schliesslich ist es ja gerade die Beurkundung durch den Notar, die die Echtheit der im Schriftstück enthaltenen Informationen bestätigen soll. Mit der Verwendung von vertrauenswürdigen, elektronischen Zertifikaten für die Anmeldung am eArchive wird sichergestellt, dass der für die Ablage und damit auch für die Echtheit verantwortliche Notar eindeutig identifiziert werden kann.

**Integrität:** Dokumente müssen zuverlässig gegen Veränderungen und Löschung geschützt werden. Nachträgliche Kommentare und Anmerkungen sind nur im Rahmen von klar definierten Policies oder Prozessen zulässig, müssen explizit ausgewiesen werden und rückverfolgbar sein. Die Integrität der abgelegten Dokumente wird etwa durch eine stringente Versionierung, die Protokollierung aller Schreib-Operationen in einem Audit-Trail, digitale Signatur des zuständigen Notars oder die eindeutige Authentisierung der Benutzer gewährleistet. Ausserdem hat AdNovum die Lösch-Funktion von Alfresco unterbunden, damit niemand Daten unwiderruflich löschen kann.

**Benutzbarkeit:** Das Schriftgut muss im Kontext seiner Erstellung gesucht und gefunden sowie in geeigneter Form ausgeliefert und dargestellt werden können. Auch muss sich ein Zusammenhang zwischen Schriftgütern herstellen lassen, die in demselben Geschäftskontext erstellt worden sind, beispielsweise indem verschiedene Verträge zum gleichen Projekt in einem elektronischen Dossier zusammengefasst werden. Über zu jedem Dokument erfasste Metadaten sowie eine Volltextsuche lassen sich Dokumente im eArchive schnell finden. Das eArchive ist redundant auf eine hohe Verfügbarkeit ausgelegt und die Dokumente sind problemlos migrierbar.

**Sicherheit:** Um die grösstmögliche Sicherheit zu gewährleisten, werden die Zugriffsrechte restriktiv verwaltet, die abgelegten Dokumente zwischen dem Speichern und der Ablage mit einem zweigeteilten Masterkey verschlüsselt sowie die Benutzer des eArchive eindeutig mit Zertifikaten authentisiert. Ausserdem erfolgt der Zugriff ausschliesslich über den gesicherten Kanal des Nevis Reverse-Proxys und alle Verbindungen zwischen den Komponenten sind mit SSL verschlüsselt.

((Highlights 400 Zeichen))

#### Highlights

- AdNovum hat ein eArchive für die Schweizer Notare entwickelt.
- Als Identitätsprovider wurde über das Security-Framework Nevis das bestehende Notaren-Register eingebunden.
- Das Rollenkonzept ermöglicht die flexible Vergabe von Zugriffsrechten und die Abbildung von Spezialfällen.
- Das Open-Source DMS Alfresco bietet eine umfassende Funktionalität und volle Kontrolle bei tiefen Kosten.

((Zitate / Entrefilets für Verteilung im Text))

Das Register dient der Identifikation der Notare über elektronische Zertifikate.

Die Verwaltung von Schriftgut verlangt besondere Funktionalitäten.

Das flexible Rollenkonzept erlaubt die feingranulare Vergabe von Zugriffsrechten.

Das Security-Framework Nevis ermöglicht einen zentralen, sicheren Zugang.

((Autorenbox Daniel Seiler & Simon Zweifel 300 Zeichen))