

Geprüfte IT-Sicherheit durch FairPay-Vorgehensmodell

Im Rahmen des vom **Bundesministerium für Wirtschaft und Technologie (BMWi)** geförderten Vorhabens **FairPay** hat das DFKI gemeinsam mit den Verbundpartnern ein Vorgehensmodell zur Entwicklung von verlässlichen Systemen des elektronischen Zahlungsverkehrs konzipiert.

Durch die Verbindung von methodischer Anleitung mit objektivierten Modellierungstechniken, zugehörigen Werkzeugen und Lösungsmustern entsteht ein Tool, das an die speziellen Bedürfnisse des Anwenders angepasst werden kann.

Sowohl für die Endnutzer wie auch die Betreiber von Systemen des elektronischen Zahlungsverkehrs geht es nicht nur um Techniken zur Entwicklung von tatsächlich sicheren Systemen, sondern auch um Verfahren zur Überprüfung von Systementwicklungen durch unabhängige Dritte, die erst begründetes Vertrauen in die Sicherheit von Lösungen schaffen. Das FairPay-Vorgehensmodell orientiert sich daher an den Anforderungen der international anerkannten „**Common Criteria for Information Technology Security Evaluation**“ (CC) zur unabhängigen Bewertung der Sicherheitsleistung von Produkten des elektronischen Zahlungsverkehrs. Es versetzt Entwickler in die Lage, die zum Teil recht hohen Anforderungen – man denke an die Diskussion über die qualifizierte elektronische Signatur – der CC in möglichst effizienter und kostengünstiger Art und Weise zu erfüllen.

Im FairPay-Vorgehensmodell sind Erkenntnisse über die Methodik zur Konstruktion verlässlicher Entwürfe im Sinne von „Best Practice“-Empfehlungen aufbereitet. Sie bilden in Form von Prozessmustern (process patterns) die Bestandteile des **FairPay-Modells**. Ein Prozessmuster beschreibt eine bewährte Vorgehensweise zur Erstellung eines klar abgegrenzten Artefakts (work product), das typischerweise ein Entwurfsmuster (design pattern) darstellt.

Die konkrete Gestalt des FairPay-Vorgehensmodells spiegelt die das Security Engineering prägende enge Verflechtung von Entwicklung und Evaluation wider. So ist jedes Artefakt sowohl an Entwicklungs- als auch an Evaluationsprozesse gekoppelt. Weil damit das Vorgehensmodell die gemeinsame Grundlage für Erstellung und Prüfung bildet, dient es auch als Hilfsmittel für die Kommunikation zwischen Entwickler und Evaluator. Durch diese Verflechtung wird die Sicherheitsqualität gesteigert und der Gesamtprozess (Entwicklung und Evaluation) beschleunigt.

Dem Benutzer präsentiert sich das **FairPay-Vorgehensmodell** als Hypertext-Dokument, das mit jedem WWW-Browser angezeigt werden kann. Die Offenheit und Flexibilität des FairPay-Vorgehensmodells ermöglicht nicht nur die Anpassung an spezifische Bedürfnisse des jeweiligen Anwenders, sondern auch die Integration in komplexe Entwicklungsumgebungen, die den Fortschritt der Entwicklung verwalten und die Projektplanung durch die Auswahl der nächsten Bearbeitungsschritte unterstützen.

Zusammen mit unseren Verbundpartnern werden wir bis Jahresende das FairPay-Vorgehensmodell für die Entwicklung und die dazugehörigen Anforderungen für die Zertifizierung von Produkten des elektronischen Zahlungsverkehrs veröffentlichen. Mit unserem **Transferzentrum SiSo - Sichere Software** stehen wir unseren Partnern und Kunden für die Umsetzung des FairPay-Vorgehensmodells bei der Entwicklung von Produkten des elektronischen Zahlungsverkehrs zur Verfügung. Gleichzeitig kann die Evaluierung durch unsere beim **Bundesamt für Sicherheit in der Informationstechnik (BSI)** akkreditierte **Prüfstelle für IT-Sicherheit** erfolgen.

Kontakt:

Dr. Oliver Keller
Email: Oliver.Keller@dfki.de
Tel.: +49 (0)681 302-5327
Fax: +49 (0)681 302-2235

